Almacenamiento de vSphere

Actualización 3
VMware vSphere 7.0
VMware ESXi 7.0
vCenter Server 7.0

vmware®

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

https://docs.vmware.com/es/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Contenido

Acerca del almacenamiento de vSphere

Almacenamiento de vSphere describe las tecnologías de almacenamiento virtualizadas y definidas por software que ofrecen VMware ESXi™ y VMware vCenter Server®, así como explicaciones sobre cómo se configuran y se usan.

En VMware, valoramos la inclusión. Para fomentar este principio dentro de nuestra comunidad de clientes, socios y personal interno, creamos contenido con un lenguaje inclusivo.

Audiencia prevista

Esta información está dirigida a administradores de sistemas con experiencia y familiarizados con las tecnologías de máquinas virtuales y virtualización de almacenamiento, las operaciones de centros de datos y los conceptos de almacenamiento SAN.

Información actualizada

Esta documentación sobre *Almacenamiento de vSphere* se actualiza con cada versión del producto o cuando sea necesario.

En esta tabla se muestra el historial de actualizaciones de *Almacenamiento de vSphere*.

Revisión	Descripción
29 de noviembre 2022	Se eliminaron las limitaciones de clúster ampliado de vSAN de Requisitos de Almacenamiento nativo en la nube y Crear una directiva de almacenamiento para Kubernetes.
28 de octubre de 2022	■ Gráfico actualizado en Ejemplo de topología de red con NVMe over TCP. ■ Actualizaciones menores en Cambiar la configuración de recuperación de espacio.
24 de agosto de 2022	Revisiones menores.
16 de agosto de 2022	Se agregó un requisito para volver a montar un almacén de datos en Cambiar la configuración de recuperación de espacio.
29 de julio de 2022	Se aclaró un requisito de grupo de replicación para la directiva de almacenamiento de Virtual Volumes en Cambiar la asignación de directivas de almacenamiento para archivos y discos de máquinas virtuales.
26 de julio de 2022	Revisiones menores.
28 de abril de 2022	Revisiones menores.
14 de diciembre de 2021	Actualizaciones menores.
29 de noviembre de 2021	Se eliminó la siguiente declaración de Complemento de alto rendimiento de VMware y esquemas de selección de rutas de acceso: "No active HPP para HDD ni dispositivos flash más lentos. No se espera que HPP proporcione beneficios de rendimiento con dispositivos que no tienen una capacidad mínima de 200 000 E/S por segundo".
17 de noviembre de 2021	Actualizaciones menores.
29 de octubre de 2021	Actualizaciones menores.
21 de octubre de 2021	Se actualizó Configurar acceso a la red para recurso compartido de archivos de vSAN para indicar que no es obligatorio usar una vNIC dedicada para el tráfico de archivos.
05 de octubre de 2021	Versión inicial.

Introducción al almacenamiento 1

vSphere admite varias opciones de almacenamiento y funcionalidades en entornos de almacenamiento tradicionales y definidos por software. Una descripción general de los aspectos y elementos de almacenamiento de vSphere de alto nivel le permite planificar una estrategia de almacenamiento adecuada a su centro de datos virtual.

Este capítulo incluye los siguientes temas:

Modelos de virtualización de almacenamiento tradicional

Por lo general, la virtualización de almacenamiento hace referencia a una abstracción lógica de los recursos de almacenamiento físico y las capacidades de las máquinas virtuales y sus aplicaciones. ESXi proporciona virtualización de almacenamiento en el nivel del host.

En el entorno de vSphere , se integra un modelo tradicional en torno a las siguientes tecnologías de almacenamiento y a las funcionalidades de virtualización de ESXi y vCenter Server.

Almacenamiento local y en red

En los entornos de almacenamiento tradicional, el proceso de administración de almacenamiento de ESXi comienza con el espacio de almacenamiento que el administrador de almacenamiento asigna previamente en los diferentes sistemas de almacenamiento. ESXi es compatible con almacenamiento en red y local.

Consulte Tipos de almacenamiento físico.

Redes de área de almacenamiento

Una red de área de almacenamiento (Storage area network, SAN) es una red de alta velocidad especializada que conecta sistemas informáticos, o hosts ESXi, con sistemas de almacenamiento de alto rendimiento. ESXi puede utilizar protocolos de canal de fibra o iSCSI para conectarse a los sistemas de almacenamiento.

Consulte Capítulo 3 Descripción general de la utilización de ESXi con una SAN.

canal de fibra

El canal de fibra (Fibre Channel, FC) es un protocolo de almacenamiento que utiliza la SAN para transferir tráfico de datos desde los servidores host ESXi hacia un almacenamiento compartido. El protocolo empaqueta comandos SCSI en tramas de canal de fibra. Para conectarse a la SAN de FC, el host usa adaptadores de bus host (Host bus adapter, HBA) de canal de fibra.

Consulte Capítulo 4 Usar ESXi con SAN de canal de fibra.

Internet SCSI

Internet iSCSI (iSCSI) es un transporte de SAN que pueden utilizar las conexiones Ethernet entre los sistemas informáticos, o hosts ESXi, y los sistemas de almacenamiento de alto rendimiento. Para conectarse a los sistemas de almacenamiento, los hosts utilizan adaptadores de iSCSI de hardware o iniciadores iSCSI de software con adaptadores de red estándar.

Consulte Capítulo 10 Usar ESXi con una SAN iSCSI.

Dispositivo de almacenamiento o LUN

En el contexto de ESXi, los términos “dispositivo” y “LUN” se utilizan indistintamente. Por lo general, ambos términos significan que se presenta un volumen de almacenamiento ante el host desde un sistema de almacenamiento en bloque y que ese volumen está disponible para darle formato.

Consulte Representar dispositivos y destinos y Capítulo 14 Administrar dispositivos de almacenamiento.

Discos virtuales

Una máquina virtual en un host ESXi utiliza un disco virtual para almacenar su sistema operativo, archivos de aplicación y otros datos relacionados con sus actividades. Los discos virtuales son archivos físicos de gran tamaño, o conjuntos de archivos, que pueden copiarse, moverse, archivarse y respaldarse con una copia de seguridad, como se haría con cualquier otro archivo. Es posible configurar máquinas virtuales con varios discos virtuales.

Para acceder a discos virtuales, una máquina virtual utiliza controladoras SCSI virtuales. Entre estas controladoras virtuales se encuentran BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS y VMware Paravirtual. Estas controladoras son los únicos tipos de controladoras SCSI que puede ver y a las que puede acceder una máquina virtual.

Cada disco virtual reside en un almacén de datos que está implementado en almacenamiento físico. Desde el punto de vista de la máquina virtual, cada disco virtual aparece como si fuera una unidad SCSI conectada a una controladora SCSI. El acceso al almacenamiento físico a través de adaptadores de almacenamiento o de red en el host generalmente es transparente para el sistema operativo invitado y las aplicaciones de la máquina virtual.

VMware vSphere® VMFS

Los almacenes de datos que se implementan en dispositivos de almacenamiento de bloques usan el formato nativo de vSphere Virtual Machine File System (VMFS). Se trata de un formato de sistema de archivos de alto rendimiento optimizado para el almacenamiento de máquinas virtuales.

Consulte Descripción de los almacenes de datos de VMFS.

NFS

Un cliente NFS integrado en ESXi utiliza el protocolo Network File System (NFS) mediante TCP/IP para acceder a un volumen NFS ubicado en un servidor NAS. El host ESXi puede montar el volumen y utilizarlo como un almacén de datos NFS.

Consulte Describir los almacenes de datos de Network File System.

Asignar dispositivos sin formato

Además de discos virtuales, vSphere ofrece un mecanismo que se conoce como asignación de dispositivos sin formato (RDM). RDM es útil para los casos donde un sistema operativo invitado dentro de una máquina virtual requiere acceso directo a un dispositivo de almacenamiento. Para obtener información sobre RDM, consulte Capítulo 19 Asignación de dispositivos sin formato.

Modelos de almacenamiento definidos por software

Además de abstraer las capacidades de almacenamiento subyacente de las máquinas virtuales, al igual que hacen los modelos de almacenamiento tradicionales, el almacenamiento definido por software abstrae las capacidades de almacenamiento.

Con el modelo de almacenamiento definido por software, una máquina virtual se convierte en una unidad de aprovisionamiento de almacenamiento y puede administrarse mediante un mecanismo basado en directivas flexible. El modelo incluye las siguientes tecnologías de vSphere .

VMware vSphere® Virtual Volumes™ (vVols)

La funcionalidad de Virtual Volumes cambia el paradigma de administración de almacenamiento de la administración del espacio interno de los almacenes de datos a la administración de objetos de almacenamiento abstractos procesados por matrices de almacenamiento. Con Virtual Volumes, una máquina virtual individual, no el almacén de datos, se convierte en una unidad de administración de almacenamiento. Por su parte, el hardware de almacenamiento tiene control total sobre el contenido, el diseño y la administración del disco virtual.

Consulte Capítulo 22 Trabajar con VMware vSphere Virtual Volumes.

VMware vSAN

vSAN es una capa distribuida de software que se ejecuta de manera nativa como parte del hipervisor. vSAN agrega dispositivos de capacidad locales o con conexión directa de un clúster de hosts ESXi y crea un grupo de almacenamiento individual compartido entre todos los hosts del clúster de vSAN.

Consulte *Administrar VMware vSAN*.

Administración de almacenamiento basada en directivas

La administración de almacenamiento basada en directivas (Storage Policy Based Management, SPBM) es un marco que proporciona un solo panel de control para varios servicios de datos y soluciones de almacenamiento, incluidos vSAN y Virtual Volumes. Mediante el uso de directivas de almacenamiento, el marco alinea las demandas de las aplicaciones de las máquinas virtuales con las capacidades proporcionadas por las entidades de almacenamiento.

Consulte Capítulo 20 Administración de almacenamiento basada en directivas.

Filtros de E/S

Los filtros de E/S son componentes de software que pueden instalarse en hosts ESXi y brindar servicios de datos adicionales a las máquinas virtuales. Según la implementación, los servicios pueden incluir replicación, cifrado, almacenamiento en caché, etc.

Consulte Capítulo 23 Filtrar E/S de máquinas virtuales.

vSphere Storage APIs

Storage APIs es una familia de API utilizada por proveedores de hardware, software y almacenamiento externos con el fin de desarrollar componentes que mejoren distintas características y soluciones de vSphere.

En esta publicación sobre almacenamiento se describen varias API de almacenamiento que favorecen el entorno de almacenamiento. Para obtener información sobre otras API de esta familia, como vSphere API - Data Protection, consulte el sitio web de VMware.

vSphere APIs for Storage Awareness

Estas API, también denominadas VASA, las suministran terceros o las ofrece VMware y proporcionan comunicación entre vCenter Server y el almacenamiento subyacente. A través de VASA, las entidades de almacenamiento pueden informar a vCenter Server sobre sus configuraciones, capacidades, y estados y eventos de almacenamiento. A cambio, VASA puede ofrecer requisitos de almacenamiento de máquina virtual de vCenter Server a una entidad de almacenamiento y garantizar que la capa de almacenamiento cumpla los requisitos.

VASA resulta esencial cuando se trabaja con Virtual Volumes, vSAN, vSphere APIs for I/O Filtering (VAIO) y directivas de máquina virtual de almacenamiento. Consulte Capítulo 21 Usar proveedores de almacenamiento.

vSphere APIs for Array Integration

Estas API, también denominadas VAAI, incluyen los siguientes componentes:

- API de aceleración de hardware. Ayuda a integrar las matrices con vSphere, de modo que vSphere pueda descargar ciertas operaciones de almacenamiento en la matriz. Esta integración reduce significativamente la sobrecarga de CPU en el host. Consulte Capítulo 24 Aceleración de hardware de almacenamiento.
- API de aprovisionamiento fino de matrices. Ayudan a supervisar la utilización del espacio en matrices de almacenamiento de aprovisionamiento fino para evitar condiciones de falta de espacio y realizar tareas de recuperación de espacio. Consulte ESXi y aprovisionamiento fino de matrices.

vSphere APIs for Multipathing

Estas API, denominadas arquitectura de almacenamiento acoplable (Pluggable Storage Architecture, PSA), permiten que los partners de almacenamiento creen y ofrezcan complementos de múltiples rutas y equilibrio de carga optimizados para cada matriz. Los complementos se comunican con las matrices de almacenamiento para establecer la mejor estrategia de selección de rutas de acceso y aumentar el rendimiento de E/S y la confiabilidad del host ESXi a la matriz de almacenamiento. Para obtener más información, consulte Administración de la ruta de acceso y arquitectura de almacenamiento acoplable.

Introducción a un modelo de almacenamiento tradicional

2

Al configurar el almacenamiento ESXi en entornos tradicionales, se incluye la configuración de los sistemas de almacenamiento y los dispositivos para habilitar los adaptadores de almacenamiento y crear almacenes de datos.

Este capítulo incluye los siguientes temas:

Tipos de almacenamiento físico

En los entornos de almacenamiento tradicional, el proceso de administración de almacenamiento de ESXi comienza con el espacio de almacenamiento que el administrador de almacenamiento asigna previamente en los diferentes sistemas de almacenamiento. ESXi es compatible con almacenamiento en red y local.

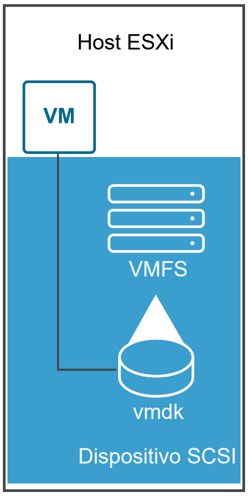
Almacenamiento local

El almacenamiento local pueden estar formado por discos duros internos que se encuentren en el host ESXi. También puede incluir sistemas de almacenamiento externos ubicados fuera y conectados al host directamente a través de protocolos como SAS o SATA.

El almacenamiento local no requiere una red de almacenamiento para comunicarse con el host. Necesita un cable conectado a la unidad de almacenamiento y, cuando se requiere, un HBA compatible en el host.

En la siguiente ilustración se muestra una máquina virtual que utiliza almacenamiento SCSI local.

Figura 2-1. Almacenamiento local



En este ejemplo de una topología de almacenamiento local, el host ESXi utiliza una sola conexión a un dispositivo de almacenamiento. En ese dispositivo, puede crear un almacén de datos de VMFS, que puede usar para almacenar archivos de disco de máquinas virtuales.

Aunque esta configuración de almacenamiento es posible, no se recomienda. Con conexiones individuales entre dispositivos de almacenamiento y hosts, se crean únicos puntos de error (SPOF) que pueden causar interrupciones cuando una conexión se vuelve poco confiable o tiene errores. Sin embargo, debido a que la mayoría de dispositivos de almacenamiento local no admiten varias conexiones, no puede usar varias rutas de acceso para acceder al almacenamiento local.

ESXi es compatible con diversos dispositivos de almacenamiento local, incluidos SCSI, IDE, SATA, USB, SAS, flash y dispositivos NVMe.

Nota No pueden usar unidades IDE/ATA o USB para almacenar máquinas virtuales.

El almacenamiento local no admite el uso de recursos compartidos entre varios hosts. Solo un host tiene acceso a un almacén de datos en un dispositivo de almacenamiento local. En consecuencia, aunque puede usar el almacenamiento local para crear máquinas virtuales, no puede utilizar las funciones de VMware que requieren almacenamiento compartido, como HA y vMotion.

Sin embargo, si usa un clúster de hosts que tienen únicamente dispositivos de almacenamiento locales, puede implementar vSAN. vSAN transforma los recursos de almacenamiento local en almacenamiento compartido definido por software. Con vSAN, puede utilizar funciones que requieren almacenamiento compartido. Para obtener información detallada, consulte la documentación de *Administrar VMware vSAN*.

Almacenamiento en red

El almacenamiento en red consiste en sistemas de almacenamiento externos que usa el host ESXi para almacenar archivos de máquina virtual de forma remota. Generalmente, el host accede a estos sistemas por medio de una red de almacenamiento de alta velocidad.

Los dispositivos de almacenamiento en red son compartidos. Varios hosts pueden acceder simultáneamente a los almacenes de datos en dispositivos de almacenamiento en red. ESXi admite varias tecnologías de almacenamiento en red.

Además del almacenamiento en red tradicional que abarca este tema, VMware admite almacenamiento compartido virtualizado, como vSAN. vSAN transforma los recursos de almacenamiento internos de los hosts ESXi en un almacenamiento compartido que brinda capacidades como High Availability y vMotion para las máquinas virtuales. Para obtener información detallada, consulte la documentación de *Administrar VMware vSAN*.

Nota No se puede presentar el mismo LUN a un host ESXi o a varios hosts a través de distintos protocolos de almacenamiento. Para acceder al LUN, los hosts deben usar siempre un solo protocolo, por ejemplo, solo canal de fibra o solo iSCSI.

Canal de fibra (FC)

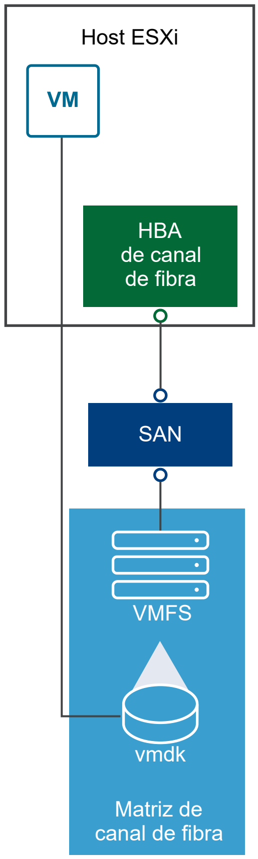
Almacena archivos de máquina virtual de forma remota en una red de área de almacenamiento (SAN) de FC. SAN de FC es una red especializada de alta velocidad que conecta los hosts a dispositivos de almacenamiento de alto rendimiento. La red usa el protocolo Fibre Channel para transportar el tráfico SCSI desde las máquinas virtuales hasta los dispositivos SAN de FC.

Para conectarse a la SAN de FC, el host debe tener adaptadores de bus host (HBA) de canal de fibra. A menos que use el almacenamiento de conexión directa de canal de fibra, necesitará conmutadores de canal de fibra para enrutar el tráfico de almacenamiento. Si el host contiene adaptadores de canal de fibra en Ethernet (FCoE), solo puede conectarse a los dispositivos de canal de fibra compartidos con una red Ethernet.

Nota A partir de vSphere 7.0, VMware deja de ser compatible con FCoE de software en entornos de producción.

El almacenamiento de canal de fibra muestra las máquinas virtuales que usan almacenamiento de canal de fibra.

Figura 2-2. Almacenamiento de canal de fibra



En esta configuración, un host se conecta a un tejido de SAN, que consiste en conmutadores de canal de fibra y matrices de almacenamiento, con un adaptador de canal de fibra. Los LUN de una matriz de almacenamiento pasan a estar disponibles para el host. Puede acceder a los LUN y crear almacenes de datos para satisfacer sus necesidades de almacenamiento. Los almacenes de datos usan el formato VMFS.

Para obtener información específica sobre la configuración de la SAN de canal de fibra, consulte Capítulo 4 Usar ESXi con SAN de canal de fibra.

Internet SCSI (iSCSI)

Almacena archivos de máquina virtual en dispositivos de almacenamiento iSCSI. iSCSI empaqueta el tráfico de almacenamiento SCSI en el protocolo TCP/IP para que pueda viajar por redes TCP/IP estándar en lugar de una red de FC especializada. Con una conexión iSCSI, el host actúa como el iniciador que se comunica con un destino, ubicado en sistemas de almacenamiento iSCSI remotos.

ESXi ofrece los tipos siguientes de conexiones iSCSI:

iSCSI de hardware

El host se conecta al almacenamiento a través de un adaptador de terceros capaz de descargar el procesamiento de red e iSCSI. Los adaptadores de hardware pueden ser dependientes e independientes.

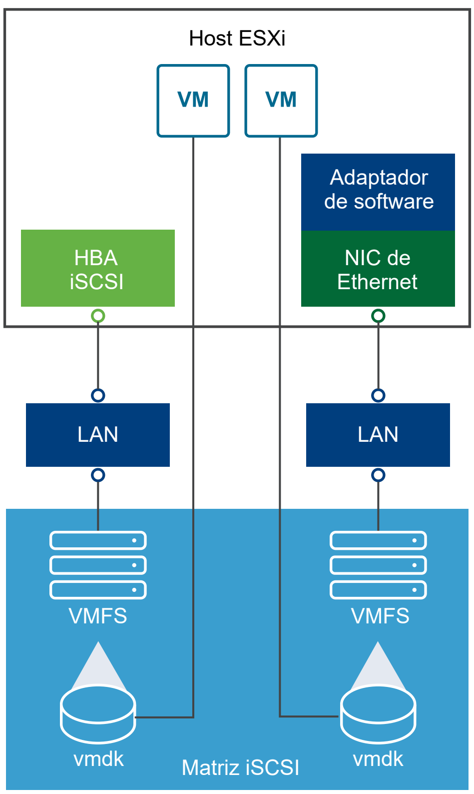
iSCSI de software

El host usa un iniciador iSCSI basado en software en VMkernel para conectarse al almacenamiento. Con este tipo de conexión iSCSI, el host necesita solo un adaptador de red estándar para la conectividad de red.

Debe configurar iniciadores iSCSI para que el host acceda y muestre los dispositivos de almacenamiento iSCSI.

El almacenamiento iSCSI muestra distintos tipos de iniciadores iSCSI.

Figura 2-3. Almacenamiento iSCSI



En el ejemplo de la izquierda, el host usa el adaptador de iSCSI de hardware para conectarse al sistema de almacenamiento iSCSI.

En el ejemplo de la derecha, el host usa un adaptador de iSCSI de software y una NIC Ethernet para conectarse al almacenamiento iSCSI.

Los dispositivos de almacenamiento iSCSI del sistema de almacenamiento pasan a estar disponibles para el host. Puede acceder a los dispositivos de almacenamiento y crear almacenes de datos de VMFS para sus necesidades de almacenamiento.

Para obtener información específica sobre la configuración de la SAN iSCSI, consulte Capítulo 10 Usar ESXi con una SAN iSCSI.

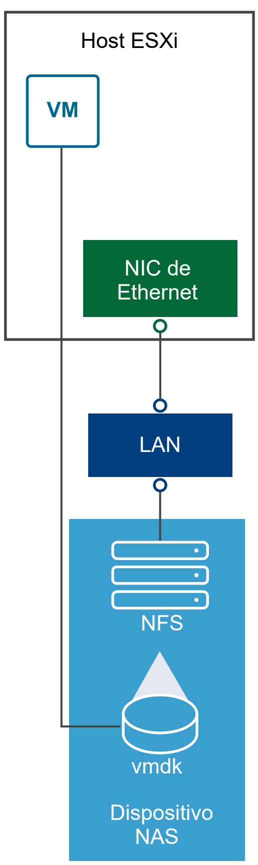
Almacenamiento conectado a la red (NAS)

Almacena los archivos de máquina virtual en servidores de archivos remotos a los que se accede a través de una red TCP/IP estándar. El cliente NFS incorporado en ESXi usa las versiones 3 y 4.1 del protocolo Network File System (NFS) para comunicarse con los servidores NAS/NFS. Para la conectividad de red, el host requiere un adaptador de red estándar.

Puede montar un volumen NFS directamente en el host ESXi. A continuación, utilice el almacén de datos NFS para almacenar y administrar las máquinas virtuales del mismo modo que con los almacenes de datos VMFS.

El almacenamiento NFS muestra una máquina virtual que usa el almacén de datos NFS para almacenar sus archivos. En esta configuración, el host se conecta al servidor NAS, que almacena los archivos de disco virtual, a través de un adaptador de red normal.

Figura 2-4. Almacenamiento NFS



Para obtener información específica sobre la configuración del almacenamiento NFS, consulte Describir los almacenes de datos de Network File System.

Shared Serial Attached SCSI (SAS)

Almacena máquinas virtuales en sistemas de almacenamiento SAS directamente conectados que ofrecen acceso compartido a varios hosts. Este tipo de acceso permite que varios hosts accedan al mismo almacén de datos de VMFS en un LUN.

Almacenamiento de NVMe over Fabrics

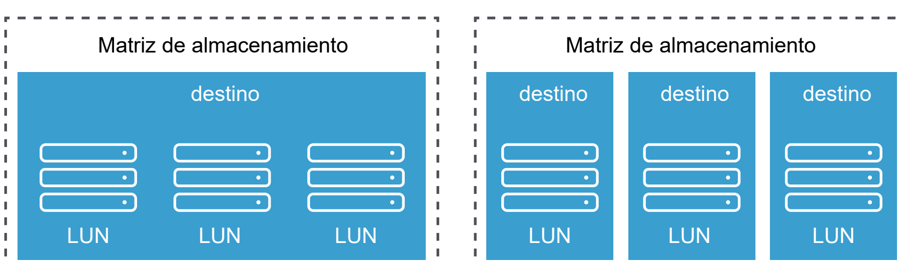
VMware NVMe over Fabrics (NVMe-oF) proporciona una conectividad a distancia entre un host y un dispositivo de almacenamiento de destino en una matriz de almacenamiento compartido. VMware admite los transportes de NVMe over RDMA (con tecnología RoCE v2), NVMe over Fibre Channel (FC-NVMe) y la tecnología NVMe over TCP/IP. Para obtener más información, consulte Capítulo 16 Acerca del almacenamiento de NVMe de VMware.

Representar dispositivos y destinos

En el contexto de ESXi, el término destino identifica a una sola unidad de almacenamiento a la que puede acceder el host. Los términos dispositivo de almacenamiento y LUN describen un volumen lógico que representa espacio de almacenamiento en un destino. En el contexto de ESXi, ambos términos representan también un volumen de almacenamiento que se presenta al host desde un destino de almacenamiento y que está disponible para cambiar su formato. Dispositivo de almacenamiento y LUN se suelen utilizar indistintamente.

Los distintos proveedores de almacenamiento presentan los sistemas de almacenamiento a los hosts ESXi de distintas formas. Algunos proveedores presentan un solo destino con varios dispositivos de almacenamiento o LUN, mientras que otros presentan varios destinos con un LUN cada uno.

Figura 2-5. Representar LUN y destinos



En esta ilustración, hay disponibles tres LUN en cada configuración. En uno de los casos, el host se conecta a un destino, pero ese destino tiene tres LUN que se pueden utilizar. Cada LUN representa un volumen de almacenamiento individual. En el otro ejemplo, el host detecta tres destinos distintos, cada uno con un LUN.

Los destinos a los que se accede a través de la red tienen nombres únicos proporcionados por los sistemas de almacenamiento. Los destinos iSCSI utilizan nombres de iSCSI, mientras que los destinos de canal de fibra utilizan nombres World Wide Names (WWN).

Nota ESXi no admite el acceso al mismo LUN a través de distintos protocolos de transporte, como iSCSI y canal de fibra.

Un dispositivo, o LUN, se identifica por su nombre de UUID. Si varios hosts comparten un LUN, debe presentarse a todos los hosts con el mismo UUID.

Acceden al almacenamiento las máquinas virtuales

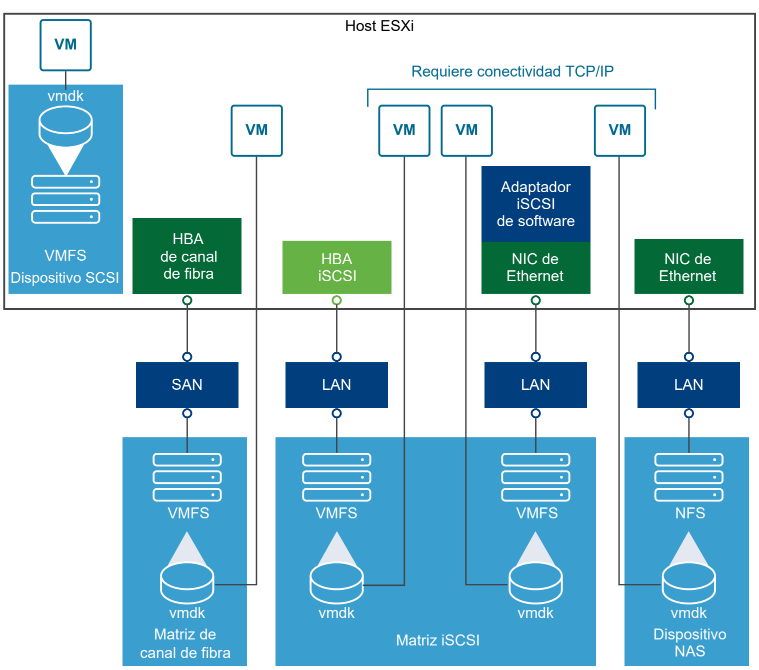
Cuando una máquina virtual se comunica con su disco virtual almacenado en un almacén de datos, emite comandos SCSI. Debido a que los almacenes de datos pueden existir en distintos tipos de almacenamiento físico, estos comandos se encapsulan en otras formas, según el protocolo que el host ESXi usa para conectarse a un dispositivo de almacenamiento.

ESXi admite los protocolos Fibre Channel (FC), Internet SCSI (iSCSI), Fibre Channel over Ethernet (FCoE) y NFS. Más allá del tipo de dispositivo de almacenamiento que utilice el host, el disco virtual siempre aparece como un dispositivo SCSI montado para la máquina virtual. El disco virtual oculta una capa de almacenamiento físico desde el sistema operativo de la máquina virtual. Esto permite ejecutar sistemas operativos que no estén certificados para equipos de almacenamiento específicos, como SAN, dentro de la máquina virtual.

Nota A partir de vSphere 7.0, VMware deja de ser compatible con FCoE de software en entornos de producción.

En el siguiente gráfico se incluyen cinco máquinas virtuales que usan diferentes tipos de almacenamiento para ilustrar las diferencias entre cada uno de ellos.

Figura 2-6. Acceso de máquinas virtuales a diferentes tipos de almacenamiento



Nota Este diagrama tiene fines exclusivamente conceptuales. No se trata de una configuración recomendada.

Características de los dispositivos de almacenamiento

Cuando el host ESXi se conecta a los sistemas de almacenamiento basado en bloques, los dispositivos de almacenamiento o LUN que admiten ESXi se vuelven disponibles para el host.

Después de registrar los dispositivos en el host, puede mostrar todos los dispositivos en red y locales que hay disponibles y revisar su información. Si se usan complementos de múltiples rutas de terceros, los dispositivos de almacenamiento disponibles por medio de los complementos también aparecen en la lista.

Nota Si una matriz admite el acceso a unidades lógicas asimétricas (Asymmetric Logical Unit Access, ALUA) implícitas y solo tiene rutas de acceso en espera, se produce un error en el registro del dispositivo. El dispositivo se puede registrar con el host después de que la instancia de destino activa una ruta de acceso en espera y el host la detecta como activa. El parámetro `/Disk/FailDiskRegistration` avanzado del sistema controla este comportamiento del host.

Se puede ver una lista independiente de los dispositivos de almacenamiento disponibles para un adaptador en particular.

Generalmente, al consultar los dispositivos de almacenamiento, se ve la siguiente información.

Tabla 2-1. Información de dispositivos de almacenamiento

Información de dispositivos de almacenamiento	Descripción
Nombre	También llamado Nombre para mostrar. Es un nombre que el host ESXi asigna al dispositivo según el tipo de almacenamiento y el fabricante. En general, puede cambiar este nombre por uno de su elección. Consulte Cambiar nombre de los dispositivos de almacenamiento.
Identificador	Un identificador universalmente único que es intrínseco al dispositivo. Consulte Identificadores y nombres de dispositivos de almacenamiento.
Estado operativo	Indica si el dispositivo está conectado o desconectado. Consulte Separar dispositivos de almacenamiento.
LUN	Número de unidad lógica (LUN) en el destino SCSI. El número LUN se obtiene del sistema de almacenamiento. Si un destino tiene un solo LUN, el número LUN siempre es cero (0).
Tipo	Tipo de dispositivo, por ejemplo, disco o CD-ROM.
Tipo de unidad	Información que especifica si el dispositivo es una unidad flash o una unidad HDD regular. Para obtener más información sobre las unidades flash y los dispositivos NVMe, consulte Capítulo 15 Trabajar con dispositivos flash.
Transporte	Protocolo de transporte que usa el host para acceder al dispositivo. El protocolo depende del tipo de almacenamiento que se usa. Consulte Tipos de almacenamiento físico.
Capacidad	Capacidad total del dispositivo de almacenamiento.
Propietario	El complemento, como NMP o el complemento de un tercero, que el host usa para administrar las rutas de acceso al dispositivo de almacenamiento. Consulte Administración de la ruta de acceso y arquitectura de almacenamiento acoplable.

Tabla 2-1. Información de dispositivos de almacenamiento (continuación)

Información de dispositivos de almacenamiento	Descripción
Aceleración de hardware	Información sobre si el dispositivo de almacenamiento asiste al host en las operaciones de administración de máquinas virtuales. El estado puede ser Compatible, No compatible o Desconocido. Consulte Capítulo 24 Aceleración de hardware de almacenamiento.
Formato de sector	Indica si el dispositivo usa un formato tradicional, 512n o de sector avanzado, como 512e o 4Kn. Consulte Formatos de sector de dispositivos.
Ubicación	Una ruta de acceso al dispositivo de almacenamiento en el directorio `/vmfs/devices/`.
Formato de partición	Un esquema de particiones que usa el dispositivo de almacenamiento. Puede ser un formato de registro de arranque maestro (Master Boot Record, MBR) o de tabla de particiones GUID (GUID partition table, GPT). Los dispositivos GPT pueden admitir almacenes de datos mayores a 2 TB. Consulte Formatos de sector de dispositivos.
Particiones	Particiones principales y lógicas, incluido un almacén de datos de VMFS, si está configurado.
Directivas de múltiples rutas	Directiva de selección de rutas de acceso y directiva de tipo de matriz de almacenamiento que usa el host para administrar las rutas de acceso al almacenamiento. Consulte Capítulo 18 Descripción de múltiples rutas y conmutación por error.
Rutas de acceso	Rutas de acceso que se utilizan para acceder al almacenamiento y a su estado. Consulte Deshabilitar rutas de acceso de almacenamiento.

Mostrar dispositivos de almacenamiento de un host ESXi

Muestre todos los dispositivos de almacenamiento disponibles para un host ESXi. Si se utiliza algún complemento de múltiples rutas de terceros, los dispositivos de almacenamiento disponibles por medio de los complementos también aparecen en la lista.

La vista Dispositivos de almacenamiento permite enumerar los dispositivos de almacenamiento de los hosts, analizar la información y modificar las propiedades.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Dispositivos de almacenamiento**.

   Todos los dispositivos de almacenamiento disponibles para el host se enumeran en la tabla Dispositivos de almacenamiento.

4 Para ver los detalles de un dispositivo específico, seleccione el dispositivo en la lista.

5 Utilice los iconos para realizar tareas de administración de almacenamiento básicas.

   La disponibilidad de ciertos iconos depende del tipo de dispositivo y de la configuración.

Icono	Descripción
Actualizar	Actualice la información sobre los adaptadores de almacenamiento, la topología y los sistemas de archivos.
Separar	Separe el dispositivo seleccionado del host.
Asociar	Asocie el dispositivo seleccionado al host.
Cambiar nombre	Cambie el nombre para mostrar del dispositivo seleccionado.
Encender LED	Encienda el LED del localizador de los dispositivos seleccionados.
Apagar LED	Apague el LED del localizador de los dispositivos seleccionados.
Marcar como discos flash	Marque los dispositivos seleccionados como discos flash.
Marcar como disco HDD	Marque los dispositivos seleccionados como discos HDD.
Marcar como local	Marque los dispositivos seleccionados como locales para el host.
Marcar como remoto	Marque los dispositivos seleccionados como remotos para el host.
Borrar particiones	Borre las particiones de los dispositivos seleccionados.
Marcar como reservado de forma perenne	Marque el dispositivo seleccionado como reservado de forma perenne.
Desmarcar como reservado de forma perenne	Borre la reserva perenne del dispositivo seleccionado.

6 Use las siguientes pestañas para acceder a información adicional y modificar las propiedades del dispositivo seleccionado.

Tabulador	Descripción
Propiedades	Vea las propiedades y características del dispositivo. Vea y modifique las directivas de múltiples rutas para el dispositivo.
Rutas de acceso	Muestre las rutas de acceso disponibles para el dispositivo. Permite deshabilitar o habilitar una ruta de acceso seleccionada.
Detalles de particiones	Muestra información sobre las particiones y sus formatos.

Mostrar dispositivos de almacenamiento para un adaptador

Muestre una lista de dispositivos de almacenamiento a los que se pueda acceder a través de un adaptador de almacenamiento específico en el host ESXi.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento**.

Todos los adaptadores de almacenamiento instalados en el host se enumeran en la tabla Adaptadores de almacenamiento.

4 Seleccione el adaptador en la lista y haga clic en la pestaña **Dispositivos**.

Aparecen los dispositivos de almacenamiento a los que puede acceder el host a través del adaptador.

5 Utilice los iconos para realizar tareas de administración de almacenamiento básicas.

La disponibilidad de ciertos iconos depende del tipo de dispositivo y de la configuración.

Icono	Descripción
Actualizar	Actualice la información sobre los adaptadores de almacenamiento, la topología y los sistemas de archivos.
Separar	Separe el dispositivo seleccionado del host.
Asociar	Asocie el dispositivo seleccionado al host.
Cambiar nombre	Cambie el nombre para mostrar del dispositivo seleccionado.

Comparar tipos de almacenamiento

La compatibilidad con ciertas funcionalidades de vSphere puede depender de la tecnología de almacenamiento utilizada.

En la siguiente tabla se comparan las tecnologías de almacenamiento en red compatibles con ESXi.

Tabla 2-2. Almacenamiento en red compatible con ESXi

Tecnología	Protocolos	Transferencias	Interfaz
canal de fibra	FC/SCSI	Acceso en bloque a datos/LUN	HBA de FC
canal de fibra en Ethernet	FCoE/SCSI	Acceso en bloque a datos/LUN	■ Adaptador de red convergente (FCoE de hardware) ■ NIC compatible con FCoE (FCoE de software) **Nota** A partir de vSphere 7.0, VMware deja de ser compatible con FCoE de software en entornos de producción.
iSCSI	IP/SCSI	Acceso en bloque a datos/LUN	■ HBA de iSCSI o NIC habilitada para iSCSI (iSCSI de hardware) ■ Adaptador de red (iSCSI de software)
NAS	IP/NFS	Archivo (sin acceso directo al LUN)	Adaptador de red

En la siguiente tabla se comparan las características de vSphere y los diferentes tipos de almacenamiento compatibles.

Tabla 2-3. Características de vSphere compatibles con el almacenamiento

Tipo de almacenamiento	Máquina virtual de arranque	vMotion	Almacén de datos	RDM	Clúster de máquina virtual	VMware HA y DRS	Storage APIs - Data Protection
Almacenamiento local	Sí	No	VMFS	No	Sí	No	Sí
canal de fibra	Sí	Sí	VMFS	Sí	Sí	Sí	Sí
iSCSI	Sí	Sí	VMFS	Sí	Sí	Sí	Sí
NAS en NFS	Sí	Sí	NFS 3 y NFS 4.1	No	No	Sí	Sí

Nota El almacenamiento local es compatible con un clúster de máquinas virtuales en un solo host (denominado sistema Cluster-in-a-box). Se requiere un disco virtual compartido. Para obtener más información sobre esta configuración, consulte la documentación de *Administrar recursos de vSphere*.

Adaptadores de almacenamiento compatibles

Los adaptadores de almacenamiento brindan conectividad al host ESXi a una red o una unidad de almacenamiento específicas.

ESXi es compatible con distintas clases de adaptadores, entre ellos, SCSI, iSCSI, RAID, canal de fibra, canal de fibra en Ethernet (FCoE) y Ethernet. ESXi accede a los adaptadores directamente a través de los controladores de dispositivos en el VMkernel.

Según el tipo de almacenamiento que se utilice, es posible que se deba habilitar y configurar un adaptador de almacenamiento en el host.

Para obtener información sobre cómo configurar adaptadores de FCoE de software, consulte Capítulo 6 Configurar el canal de fibra en Ethernet.

Para obtener información sobre cómo configurar distintos tipos de adaptadores de iSCSI, consulte Capítulo 11 Configurar adaptadores y almacenamiento de iSCSI e iSER.

Nota A partir de vSphere 7.0, VMware deja de ser compatible con FCoE de software en entornos de producción.

Ver información sobre adaptador de almacenamiento

Un host ESXi utiliza adaptadores de almacenamiento para acceder a los diferentes dispositivos de almacenamiento. Es posible mostrar detalles de los adaptadores de almacenamiento disponibles y revisar su información.

Requisitos previos

Debe habilitar ciertos adaptadores, por ejemplo, iSCSI o FCoE de software, antes de poder ver su información. Para configurar los adaptadores, consulte la siguiente información:

- Capítulo 11 Configurar adaptadores y almacenamiento de iSCSI e iSER
- Capítulo 6 Configurar el canal de fibra en Ethernet

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento**.

4 Utilice los iconos para realizar tareas del adaptador de almacenamiento.

La disponibilidad de los iconos específicos depende de la configuración de almacenamiento.

Icono	Descripción
Agregar adaptador de software	Permite agregar un adaptador de almacenamiento. Se aplica a iSCSI de software y FCoE de software.
Actualizar	Permite actualizar la información sobre adaptadores de almacenamiento, la topología y los sistemas de archivos en el host.
Volver a examinar almacenamiento	Vuelva a examinar todos los adaptadores de almacenamiento del host para detectar dispositivos de almacenamiento o almacenes de datos de VMFS agregados recientemente.
Volver a examinar adaptador	Permite volver a examinar el adaptador seleccionado para detectar los dispositivos de almacenamiento recién agregados.

5 Para ver los detalles de un adaptador específico, seleccione el adaptador en la lista.

6 Utilice las pestañas en Detalles del adaptador para acceder a información adicional y modificar las propiedades del adaptador seleccionado.

Tabulador	Descripción
Propiedades	Permite revisar las propiedades generales del adaptador que suelen incluir un nombre y el modelo del adaptador, así como los identificadores únicos formados según los estándares del almacenamiento específico. Para los adaptadores iSCSI y FCoE, utilice esta pestaña a fin de configurar propiedades adicionales, como la autenticación.
Dispositivos	Permite ver los dispositivos de almacenamiento a los que puede acceder el adaptador. Utilice la pestaña para realizar tareas básicas de administración de dispositivos. Consulte Mostrar dispositivos de almacenamiento para un adaptador.
Rutas de acceso	Enumera y administra todas las rutas de acceso que utiliza el adaptador para acceder a los dispositivos de almacenamiento.
Destinos (canal de fibra e iSCSI)	Permite revisar y administrar los destinos a los que se accede a través del adaptador.

Tabulador	Descripción
Enlace de puertos de red (solo para iSCSI)	Configura el enlace de puertos para adaptadores de iSCSI de hardware dependiente y software.
Opciones avanzadas (solo para iSCSI)	Configura los parámetros avanzados de iSCSI.

Características de los almacenes de datos

Los almacenes de datos son contenedores lógicos, de manera análoga a los sistemas de archivos, que ocultan aspectos específicos de cada dispositivo de almacenamiento y ofrecen un modelo uniforme para almacenar archivos de máquinas virtuales. Puede visualizar todos los almacenes de datos disponibles para los hosts y analizar sus propiedades.

Los almacenes de datos se agregan a vCenter Server mediante los siguientes métodos:

- Puede crear un almacén de datos VMFS, un almacén de datos de NFS versión 3 o 4.1, o un almacén de datos de Virtual Volumes mediante el asistente Nuevo almacén de datos. Un almacén de datos de vSAN se crea automáticamente cuando se habilita vSAN.
- Cuando agrega un host ESXi a vCenter Server, todos los almacenes de datos del host se agregan a vCenter Server.

En la siguiente tabla, se describen los detalles de almacén de datos que puede consultar al revisar los almacenes de datos desde vSphere Client. Es posible que ciertas características no estén disponibles o no sean aplicables para todos los tipos de almacenes de datos.

Tabla 2-4. Información de almacén de datos

Información de almacén de datos	Tipo de almacén de datos aplicable	Descripción
Nombre	VMFS NFS vSAN vVol	Nombre editable que se asigna a un almacén de datos. Para obtener información sobre el cambio de nombre de un almacén de datos, consulte Cambiar nombre del almacén de datos.
Tipo	VMFS NFS vSAN vVol	El sistema de archivos que usa el almacén de datos. Para obtener información sobre los almacenes de datos de VMFS y NFS, y el modo de administrarlos, consulte Capítulo 17 Trabajar con almacenes de datos. Para obtener información sobre los almacenes de datos de vSAN, consulte la documentación de *Administrar VMware vSAN*. Para obtener información sobre Virtual Volumes, consulte Capítulo 22 Trabajar con VMware vSphere Virtual Volumes.
Copia de seguridad de los dispositivos	VMFS NFS vSAN	Información sobre el almacenamiento subyacente, como un dispositivo de almacenamiento en el que se implementan el almacén de datos (VMFS), el servidor y la carpeta (NFS), o los grupos de discos (vSAN).

Tabla 2-4. Información de almacén de datos (continuación)

Información de almacén de datos	Tipo de almacén de datos aplicable	Descripción
Extremos de protocolo	vVol	Información sobre los extremos de protocolo correspondientes. Consulte Extremos de protocolo.
Extensiones	VMFS	Extensiones individuales que expanden el almacén de datos y su capacidad.
Tipo de unidad	VMFS	Tipo de dispositivo de almacenamiento subyacente, como una unidad flash o una unidad HHD regular. Para obtener información detallada, consulte Capítulo 15 Trabajar con dispositivos flash.
Capacidad	VMFS NFS vSAN vVol	Incluye capacidad total, espacio aprovisionado y espacio libre.
Punto de montaje	VMFS NFS vSAN vVol	Una ruta de acceso al almacén de datos en el directorio `/vmfs/volumes/` del host.
Conjunto de funcionalidades	VMFS **Nota** Un almacén de datos de VMFS de varias extensiones asume las funcionalidades de solo una de sus extensiones. NFS vSAN vVol	Información sobre los servicios de datos de almacenamiento que proporciona la entidad de almacenamiento subyacente. No se pueden modificar.
Storage I/O Control	VMFS NFS	Información sobre el estado de la priorización de E/S de almacenamiento en todo el clúster, para saber si está habilitada o no. Consulte la documentación de *Administrar recursos de vSphere*.
Aceleración de hardware	VMFS NFS vSAN vVol	Información sobre la compatibilidad de la entidad de almacenamiento subyacente con la aceleración de hardware. El estado puede ser Compatible, No compatible o Desconocido. Para obtener información detallada, consulte Capítulo 24 Aceleración de hardware de almacenamiento. **Nota** NFS 4.1 no admite la aceleración de hardware.
Etiquetas	VMFS NFS vSAN vVol	Las funcionalidades de bases de datos que el usuario define y asocia con almacenes de datos en forma de etiquetas. Para obtener información, consulte Asignar etiquetas a almacenes de datos.

Tabla 2-4. Información de almacén de datos (continuación)

Información de almacén de datos	Tipo de almacén de datos aplicable	Descripción
Conectividad con hosts	VMFS NFS vVol	Hosts en los que está montado el almacén de datos.
Múltiples rutas	VMFS vVol	Directiva de selección de rutas de acceso que usa el host para acceder al almacenamiento. Para obtener más información, consulte Capítulo 18 Descripción de múltiples rutas y conmutación por error.

Mostrar la información del almacén de datos

Acceda a la vista Almacenes de datos con el navegador de vSphere Client.

Use la vista Almacenes de datos para enumerar todos los almacenes de datos disponibles en el inventario de infraestructura de vSphere, analizar la información y modificar las propiedades.

Procedimiento

1 Desplácese hasta cualquier objeto de inventario que sea un objeto principal válido de un almacén de datos, por ejemplo, un host, un clúster o un centro de datos y haga clic en la pestaña **Almacenes de datos**.

   Los almacenes de datos que están disponibles en el inventario aparecen en el panel central.

2 Use las opciones de un menú contextual del almacén de datos para realizar tareas básicas en un almacén seleccionado.

   La disponibilidad de opciones específicas depende del tipo de almacén de datos y su configuración.

Opción	Descripción
Registrar máquina virtual	Registra una máquina virtual existente en el inventario. Consulte la documentación de *Administrar máquinas virtuales de vSphere*.
Aumentar capacidad del almacén de datos	Aumente la capacidad del almacén de datos VMFS o agregue una extensión. Consulte Aumentar la capacidad de un almacén de datos de VMFS.
Examinar archivos	Permite desplazarse hasta el explorador de archivos en el almacén de datos. Consulte Usar el explorador del almacén de datos.
Cambiar nombre	Cambiar el nombre del almacén de datos. Consulte Cambiar nombre del almacén de datos.
Montar almacén de datos	Monte el almacén de datos en ciertos hosts. Consulte Montar almacenes de datos.
Desmontar almacén de datos	Desmonte el almacén de datos de ciertos hosts. Consulte Desmontar almacenes de datos.
Modo de mantenimiento	Use el modo de mantenimiento del almacén de datos. Consulte la documentación de *Administrar recursos de vSphere*.

Opción	Descripción
Configurar Storage I/O Control (VMFS)	Habilite Storage I/O Control para el almacén de datos VMFS. Consulte la documentación de *Administrar recursos de vSphere*.
Editar recuperación de espacio (VMFS)	Cambie la configuración de recuperación de espacio del almacén de datos VMFS. Consulte Cambiar la configuración de recuperación de espacio.
Eliminar almacén de datos (VMFS)	Elimine el almacén de datos VMFS. Consulte Quitar almacenes de datos de VMFS.
Etiquetas y atributos personalizados	Use etiquetas para codificar información sobre el almacén de datos. Consulte Asignar etiquetas a almacenes de datos.

3 Para ver detalles específicos del almacén de datos, haga clic en el almacén de datos seleccionado.

4 Utilice las pestañas para acceder a la información adicional y modificar las propiedades del almacén de datos.

Tabulador	Descripción
Resumen	Vea las estadísticas y la configuración de los almacenes de datos seleccionados.
Supervisar	Vea la información sobre alarmas, datos de rendimiento, asignación de recursos, eventos y otra información de estado del almacén de datos.
Configurar	Vea y modifique las propiedades del almacén de datos. Los elementos de menú visibles dependen del tipo de almacén de datos.
Permisos	Asigne o modifique los permisos del almacén de datos seleccionado.
Archivos	Permite desplazarse hasta el explorador de archivos en el almacén de datos.
Hosts	Vea los hosts en los que está montado el almacén de datos.
Máquinas virtuales	Vea las máquinas virtuales que residen en el almacén de datos.

Usar dispositivos de memoria persistente con ESXi

ESXi es compatible con dispositivos de memoria persistente de última generación, también conocidos como dispositivos de memoria no volátil (Non-Volatile Memory, NVM). Estos dispositivos combinan el rendimiento y la velocidad de memoria con la persistencia del almacenamiento tradicional. Pueden conservar los datos almacenados aunque ocurran reinicios o fallas en la fuente de alimentación.

Las máquinas virtuales que requieren persistencia, baja latencia y gran ancho de banda pueden beneficiarse con esta tecnología. Algunos ejemplos son las máquinas virtuales con carga de trabajo de análisis y bases de datos de aceleración.

Para utilizar la memoria persistente en un host ESXi, debe estar familiarizado con los siguientes conceptos.

Almacén de datos PMem

Después de agregar memoria persistente al host ESXi, este detecta el hardware y, a continuación, se formatea y se monta como un almacén de datos PMem local. ESXi utiliza

VMFS-L como formato de sistema de archivos. Se admite solo un almacén de datos PMem local en cada host.

Nota Al administrar memoria persistente física, asegúrese de evacuar todas las máquinas virtuales del host y coloque el host en modo de mantenimiento.

Para reducir la sobrecarga administrativa, el almacén de datos PMem ofrece un modelo de administración simplificada. Por lo general, las tareas de un almacén de datos tradicional no se aplican al almacén de datos debido a que el host realiza automáticamente todas las operaciones necesarias en segundo plano. Como administrador, no se puede mostrar el almacén de datos en la vista Almacenes de datos de vSphere Client ni realizar otras acciones normales en el almacén de datos. La única operación disponible es la supervisión de estadísticas del almacén de datos PMem.

El almacén de datos PMem se utiliza para almacenar los dispositivos NVDIMM virtuales y los discos virtuales tradicionales de una máquina virtual. El directorio principal de la máquina virtual con los archivos `vmx` y `vmware.log` no se puede colocar en el almacén de datos PMem.

Modos de acceso a PMem

ESXi expone la memoria persistente a una máquina virtual de dos modos diferentes. Las máquinas virtuales con reconocimiento PMem pueden tener acceso directo a la memoria persistente. Las máquinas virtuales tradicionales pueden utilizar discos virtuales rápidos guardados en el almacén de datos PMem.

Modo de acceso directo

En este modo, también denominado modo PMem virtual (vPMem), una región de PMem puede presentarse a una máquina virtual como un módulo virtual de memoria en línea dual no volátil (Non-Volatile Dual In-Line Memory Module, NVDIMM). La máquina virtual utiliza el módulo NVDIMM como una memoria estándar direccionable en bytes que puede ser persistente durante los ciclos de energía.

Es posible agregar uno o varios módulos NVDIMM al aprovisionar la máquina virtual.

Las máquinas virtuales deben tener las versiones de hardware ESXi 6.7 o posteriores, y un sistema operativo invitado con reconocimiento PMem. El dispositivo NVDIMM es compatible con los últimos sistemas operativos invitados que admiten memoria persistente, por ejemplo, Windows 2016.

Cada dispositivo NVDIMM se almacena automáticamente en el almacén de datos PMem.

Modo de disco virtual

Este modo, también denominado modo de discos PMem virtuales (vPMemDisk), está disponible para todas las máquinas virtuales tradicionales y es compatible con cualquier versión de hardware, incluidas todas las versiones heredadas. No es necesario que las máquinas virtuales tengan reconocimiento PMem. Cuando se usa este modo, se crea un disco

virtual normal de SCSI y se le asocia una directiva de almacenamiento de máquina virtual con PMem. La directiva coloca el disco en el almacén de datos PMem automáticamente.

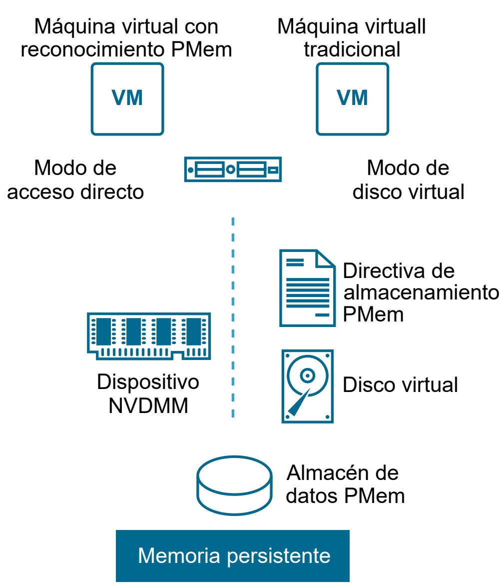
Directiva de almacenamiento PMem

Para colocar el disco virtual en el almacén de datos PMem, debe aplicar en el disco la directiva de almacenamiento PMem de host local predeterminada. La directiva no puede editarse

y solo puede aplicarse a los discos virtuales. Debido a que el directorio de inicio de la máquina virtual no reside en el almacén de datos PMem, asegúrese de colocarlo en un almacén de datos estándar.

Una vez asignada la directiva de almacenamiento de PMem al disco virtual, no se puede cambiar la directiva en el cuadro de diálogo **Configuración de edición de máquina virtual**. Para cambiarla, migre o clone la máquina virtual.

En el gráfico siguiente, se ilustra cómo interactúan los componentes de la memoria persistente.



Para obtener información acerca de cómo configurar y administrar máquinas virtuales con dispositivos NVDIMM o discos virtuales de memoria persistente, consulte la documentación de *Administrar recursos de vSphere* y *Administrar máquinas virtuales de vSphere*.

Supervisar estadísticas de almacén de datos PMem

Puede utilizar vSphere Client y el comando `esxcli` para revisar la capacidad de un almacén de datos PMem y algunos de sus otros atributos.

Sin embargo, a diferencia de los almacenes de datos regulares, como VMFS o vVol, el almacén de datos PMem no aparece en la vista Almacenes de datos de vSphere Client. Las tareas administrativas de los almacenes de datos regulares no se aplican a este almacén.

Procedimiento

- Revise la información sobre el almacén de datos PMem.

Opción	Descripción
vSphere Client	a Desplácese hasta el host ESXi y haga clic en **Resumen**. b En el panel Hardware, compruebe que se muestre la memoria persistente y revise su capacidad.
Comando esxcli	Use `esxcli storage filesystem list` para enumerar el almacén de datos PMem.

Ejemplo: Ver el almacén de datos PMem

La siguiente salida de muestra aparece cuando se usa el comando `esxcli storage filesystem list` para enumerar el almacén de datos.

```
# esxcli storage filesystem list
Mount Point              Volume Name          UUID          Mounted   Type      Size
Free
----------------------  ----------------  -------------  -------- ------- ------------
------------

/vmfs/volumes/5xxx...     ds01-102         5xxx...       true     VMFS-6  14227079168
12718178304
/vmfs/volumes/59ex...     ds02-102         59ex...       true     VMFS-6  21206401024
19697500160
/vmfs/volumes/59bx...                      59bx...       true     vfat    4293591040
4274847744
/vmfs/volumes/pmem:5ax... PMemDS-56ax...   pmem:5a0x...  true     PMEM    12880707584
11504975872
```

Descripción general de la utilización de ESXi con una SAN

3

Utilizar ESXi con una SAN mejora la flexibilidad, la eficiencia y la confiabilidad. El uso de ESXi con una SAN también es compatible con las tecnologías de equilibrio de la carga, conmutación por error y administración centralizada.

A continuación, se mencionan los beneficios de utilizar ESXi con una SAN:

- Puede almacenar datos de forma segura y configurar varias rutas de acceso al almacenamiento, y eliminar así un único punto de error.
- Utilizar una SAN con sistemas ESXi amplía la resistencia a errores al servidor. Cuando se utiliza el almacenamiento de SAN, todas las aplicaciones pueden reiniciarse instantáneamente en otro host después de un error del host original.
- Puede realizar una migración en vivo de máquinas virtuales con VMware vMotion.
- Utilice VMware High Availability (HA) junto con una SAN para reiniciar las máquinas virtuales en su último estado conocido en un servidor distinto si hay un error en su host.
- Utilice VMware Fault Tolerance (FT) para replicar máquinas virtuales protegidas en dos hosts distintos. Las máquinas virtuales siguen funcionando sin interrupción en el host secundario si ocurre un error en el principal.
- Utilice VMware Distributed Resource Scheduler (DRS) para migrar máquinas virtuales de un host a otro para el equilibrio de la carga. Como el almacenamiento está en una matriz SAN compartida, las aplicaciones continúan ejecutándose sin problemas.
- Si utiliza clústeres de VMware DRS, ponga un host ESXi en modo de mantenimiento para que el sistema migre todas las máquinas virtuales en ejecución a otros hosts ESXi. A continuación, podrá realizar actualizaciones u otras operaciones de mantenimiento en el host original.

La portabilidad y la encapsulación de máquinas virtuales de VMware complementan la naturaleza de uso compartido de este almacenamiento. Cuando las máquinas virtuales se encuentran en un almacenamiento basado en SAN, puede apagar rápidamente una máquina virtual en un servidor y prenderla en otro, o suspenderla en uno y reanudar la operación en otro servidor en la misma red. Esta capacidad permite migrar los recursos informáticos y mantener un acceso compartido coherente.

Este capítulo incluye los siguientes temas:

Casos de uso de ESXi y SAN

Cuando se utiliza con una SAN, ESXi puede aprovechar varias características de vSphere, incluidas Storage vMotion, Distributed Resource Scheduler (DRS), High Availability, etc.

La utilización de ESXi con una SAN es eficaz para las tareas siguientes:

Consolidación del almacenamiento y simplificación del diseño de almacenamiento

Si trabaja con varios hosts y cada uno ejecuta varias máquinas virtuales, el almacenamiento de los hosts deja de ser suficiente. Es posible que deba utilizar almacenamiento externo. La SAN puede proporcionar una arquitectura de sistema simple y otras ventajas.

Mantenimiento con cero tiempo de inactividad

Cuando realice mantenimiento de infraestructura o host ESXi, utilice vMotion para migrar las máquinas virtuales a otro host. Si el almacenamiento compartido está en la SAN, puede realizar el mantenimiento sin interrupciones para los usuarios de las máquinas virtuales. Los procesos en funcionamiento de la máquina virtual continúan durante toda una migración.

Equilibrio de carga

Puede agregar un host a un clúster DRS y los recursos del host se vuelven parte de los recursos del clúster. La distribución y el uso de los recursos de memoria y de CPU de todos los hosts y las máquinas virtuales en el clúster se supervisan continuamente. DRS compara estas métricas con un uso de recursos ideal. El uso ideal tiene en cuenta los atributos de las máquinas virtuales y los grupos de recursos del clúster, la demanda actual y el destino de desequilibrio. Si es necesario, DRS realizará o recomendará migraciones de máquina virtual.

Recuperación ante desastres

Puede utilizar VMware High Availability para configurar varios hosts ESXi como un clúster. El clúster ofrece una rápida recuperación frente a las interrupciones y una alta disponibilidad rentable para las aplicaciones que se ejecutan en las máquinas virtuales.

Migraciones de matrices simplificadas y actualizaciones de almacenamiento

Al adquirir nuevos sistemas de almacenamiento, se puede utilizar Storage vMotion para realizar migraciones de máquinas virtuales del almacenamiento existente a sus nuevos destinos. Puede realizar las migraciones sin interrupciones en las máquinas virtuales.

Detalles de la utilización de almacenamiento SAN con ESXi

El uso de una SAN con un host ESXi es diferente del uso de una SAN tradicional en varios aspectos.

Cuando se utiliza el almacenamiento de SAN con ESXi, se tienen en cuenta las siguientes consideraciones:

- No se pueden utilizar las herramientas de administración de SAN para acceder a los sistemas operativos de las máquinas virtuales que residen en ese almacenamiento. Con herramientas tradicionales, puede supervisar solo el sistema operativo de VMware ESXi. Puede utilizar vSphere Client para supervisar máquinas virtuales.
- El HBA visible para las herramientas de administración de SAN forma parte del sistema ESXi, no de la máquina virtual.
- Por lo general, el sistema ESXi se encarga de las múltiples rutas.

Hosts ESXi y varias matrices de almacenamiento

Un host ESXi puede acceder a dispositivos de almacenamiento presentados desde varias matrices de almacenamiento, incluidas matrices de distintos proveedores.

Cuando se utilizan varias matrices de distintos proveedores, se deben tener en cuenta las siguientes consideraciones:

- Si el host utiliza el mismo SATP para varias matrices, tenga cuidado al cambiar el PSP predeterminado para ese SATP. El cambio se aplica a todas las matrices. Para obtener información sobre SATP y PSP, consulte Capítulo 18 Descripción de múltiples rutas y conmutación por error.
- Algunas matrices de almacenamiento ofrecen recomendaciones sobre la profundidad de la cola y otras opciones. Por lo general, estas opciones se configuran de manera global en el nivel del host ESXi. Los cambios que se realizan en una matriz afectan a otras matrices que presentan LUN al host. Para obtener información sobre cómo cambiar la profundidad de la cola, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/1267.
- Utilice la división en zonas de un solo destino y un solo iniciador cuando divida en zonas los hosts ESXi en matrices de canal de fibra. Con este tipo de configuración, los eventos relacionados con el tejido que ocurren en una matriz no afectan a otras matrices. Para obtener más información sobre la división en zonas, consulte Usar la división en zonas con las SAN de canal de fibra.

Toma de decisiones relacionadas con el LUN

Debe planificar de qué forma se realizará la configuración del almacenamiento para los sistemas ESXi antes de formatear los LUN con almacenes de datos de VMFS.

Al elegir LUN, se deben tener en cuenta las siguientes consideraciones:

- Cada LUN debe tener el nivel de RAID y la característica de almacenamiento correctos para las aplicaciones que se ejecutan en las máquinas virtuales que utilizan el LUN.
- Cada LUN debe contener un solo almacén de datos de VMFS.
- Si varias máquinas virtuales acceden al mismo VMFS, utilice discos compartidos para priorizarlas.

Es conveniente tener menos LUN de mayor tamaño por los siguientes motivos:

- Más flexibilidad para crear máquinas virtuales sin solicitar más espacio al administrador de almacenamiento.
- Más flexibilidad para redimensionar los discos virtuales, realizar las snapshots, etc.
- Menos almacenes de datos de VMFS para administrar.

Es conveniente tener más LUN de menor tamaño por los siguientes motivos:

- Menos espacio de almacenamiento desperdiciado.
- Diferentes aplicaciones pueden necesitar diferentes características de RAID.
- Más flexibilidad, ya que la directiva de múltiples rutas y los discos compartidos se establecen por LUN.
- La utilización del Servicio de clúster de Microsoft requiere que cada recurso de disco de clúster esté en su propio LUN.
- Mejor rendimiento, ya que hay menos contención para un solo volumen.

Cuando la caracterización del almacenamiento de una máquina virtual no está disponible, es posible que no sea fácil determinar el número de LUN para aprovisionar y su tamaño. Puede experimentar con un esquema predictivo o adaptativo.

Usar el esquema predictivo para tomar decisiones sobre LUN

Cuando configura el almacenamiento de sistemas ESXi, antes de crear almacenes de datos de VMFS, debe decidir el tamaño y la cantidad de LUN que aprovisionará. Puede experimentar con el esquema predictivo.

Procedimiento

1. Aprovisione varios LUN con distintas características de almacenamiento.
2. Cree un almacén de datos de VMFS en cada LUN, etiquete cada almacén de datos según sus características.
3. Cree discos virtuales para contener los datos de las aplicaciones de máquina virtual en los almacenes de datos de VMFS creados en LUN con el nivel RAID adecuado para los requisitos de las aplicaciones.

4 Utilice los discos compartidos para distinguir las máquinas virtuales con prioridad alta de aquellas con prioridad baja.

Nota Los discos compartidos solo son pertinentes dentro de un host determinado. Los recursos compartidos asignados a las máquinas virtuales de un host no afectan a las máquinas virtuales de los demás hosts.

---

5 Ejecute las aplicaciones para determinar si el rendimiento de una máquina virtual es aceptable.

Usar el esquema adaptativo para tomar decisiones de LUN

Al configurar el almacenamiento para hosts ESXi, antes de crear almacenes de datos de VMFS, debe decidir el tamaño y la cantidad de LUN que aprovisionará. Puede experimentar con el esquema adaptativo.

Procedimiento

1 Aprovisione un LUN de gran tamaño (RAID 1+0 o RAID 5) con la escritura de almacenamiento en caché habilitada.

2 Cree un VMFS en ese LUN.

3 Cree cuatro o cinco discos virtuales en el VMFS.

4 Ejecute las aplicaciones para determinar si el rendimiento de un disco es aceptable.

Resultados

Si el rendimiento es aceptable, puede colocar discos virtuales adicionales en el VMFS. Si el rendimiento no es aceptable, cree un nuevo LUN de gran tamaño, posiblemente con un nivel de RAID diferente, y repita el proceso. Utilice la migración para no perder datos de máquinas virtuales al volver a crear el LUN.

Seleccionar las ubicaciones de las máquinas virtuales

Cuando se trabaja para optimizar el rendimiento de las máquinas virtuales, la ubicación del almacenamiento es un factor importante. Según cuáles sean sus necesidades de almacenamiento, podrá seleccionar un almacenamiento con alto rendimiento y alta disponibilidad o bien un almacenamiento con un rendimiento más bajo.

El almacenamiento puede dividirse en diferentes niveles de acuerdo con diversos factores:

- Nivel alto. Ofrece alto rendimiento y alta disponibilidad. Puede ofrecer snapshots integradas para facilitar la creación de copias de seguridad y las restauraciones en un punto en el tiempo (PiT). Admite replicación, redundancia completa del procesador de almacenamiento y unidades SAS. Utiliza cabezales de alto costo.
- Nivel medio. Ofrece rendimiento medio, menor disponibilidad, redundancia parcial del procesador de almacenamiento y unidades SCSI o SAS. Podría ofrecer instantáneas. Utiliza cabezales de costo intermedio.

- Nivel inferior. Ofrece bajo rendimiento y poca redundancia de almacenamiento interno. Utiliza SATA o unidades SCSI lentas.

No todas las máquinas virtuales deben estar en el almacenamiento de mayor rendimiento y disponibilidad durante todo su ciclo de vida.

Cuando se decide dónde se va a colocar una máquina virtual, se aplican las siguientes consideraciones:

- Gravedad de la máquina virtual
- Requisitos de rendimiento y disponibilidad
- Requisitos de restauración en PiT
- Requisitos de copia de seguridad y replicación

Una máquina virtual puede cambiar de nivel durante su ciclo de vida a consecuencia de los cambios que se producen en el nivel de gravedad o en la tecnología. El nivel de gravedad es relativo y puede cambiar por distintos motivos; entre ellos, por cambios en la organización, procesos operativos, requisitos normativos, planificación ante desastres, etc.

Aplicaciones de administración de terceros

Puede usar aplicaciones de administración de terceros con el host ESXi.

La mayor parte del hardware de SAN incluye el software de administración de almacenamiento. En muchos casos, este software es una aplicación web que puede usarse con cualquier explorador web conectado a la red. En otros casos, este software se suele ejecutar en el sistema de almacenamiento o en un servidor individual independiente de los servidores que utilizan SAN para fines de almacenamiento.

Puede usar el software de administración de terceros para las siguientes tareas:

- Administración de matrices de almacenamiento, como creación de LUN, administración de memorias caché de matriz, asignación de LUN y seguridad de LUN.
- Configurar replicación, puntos de control, snapshots o creación de reflejo.

Si ejecuta el software de administración de SAN en una máquina virtual, obtendrá los beneficios de una máquina virtual, incluida la conmutación por error mediante vMotion y VMware HA. Sin embargo, debido al nivel adicional de direccionamiento indirecto, es posible que el software de administración no detecte la SAN. En este caso, se puede usar un RDM.

Nota Según el sistema de almacenamiento específico, una máquina virtual puede o no ejecutar el software de administración.

Consideraciones sobre copias de seguridad de almacenamiento SAN

Contar con una estrategia de copias de seguridad adecuada es uno de los aspectos más importantes de la administración de SAN. En el entorno de SAN, las copias de seguridad tienen dos objetivos. El primer objetivo es archivar los datos en línea en un soporte físico sin conexión. Este proceso se repite periódicamente para todos los datos en línea en una programación cronológica. El segundo objetivo es proporcionar acceso a los datos sin conexión para la recuperación frente a un problema. Por ejemplo, la recuperación de la base de datos, por lo general, requiere la recuperación de archivos de registro archivados que actualmente no están en línea.

La programación de una copia de seguridad depende de varios factores:

- La identificación de aplicaciones críticas que requieren ciclos de copia de seguridad más frecuentes dentro de un período determinado.
- Los objetivos de punto de recuperación y tiempo de recuperación. Evalúe qué tan preciso debe ser el punto de recuperación y cuánto tiempo está dispuesto a esperar por él.
- La tasa de cambio (RoC) asociada con los datos. Por ejemplo, si utiliza la replicación sincrónica/asincrónica, la RoC afecta la cantidad de ancho de banda necesaria entre los dispositivos de almacenamiento principales y secundarios.
- El impacto general en un entorno de SAN, el rendimiento del almacenamiento y otras aplicaciones.
- La identificación de períodos de tráfico pico en la SAN. Las copias de seguridad programadas durante esos períodos pico pueden ralentizar las aplicaciones y el proceso de copia de seguridad.
- El tiempo para programar todas las copias de seguridad en el centro de datos.
- El tiempo que demora realizar una copia de seguridad de una aplicación individual.
- La disponibilidad de los recursos para el archivo de datos, como el acceso al soporte físico sin conexión.

Incluya un objetivo de tiempo de recuperación para cada aplicación cuando diseñe la estrategia de copia de seguridad. Es decir, tenga en cuenta el tiempo y los recursos necesarios para realizar una copia de seguridad. Por ejemplo, si una copia de seguridad programada almacena tantos datos que la recuperación requiere una cantidad de tiempo considerable, examine la copia de seguridad programada. Realice la copia de seguridad con más frecuencia, para que la copia de seguridad que se haga incluya menos datos por vez y disminuya así el tiempo de recuperación.

Si una aplicación requiere la recuperación dentro de un marco de tiempo determinado, el proceso de copia de seguridad debe proporcionar una programación cronológica y un procesamiento de datos específicos para cumplir con este requisito. La recuperación rápida puede requerir el uso de los volúmenes de recuperación que residen en el almacenamiento en línea. Este proceso le ayuda a minimizar o eliminar la necesidad de acceder a soporte físico sin conexión lento para los componentes de datos que faltan.

Usar paquetes de copia de seguridad de terceros

Es posible utilizar soluciones de copia de seguridad de terceros para proteger los datos del sistema, de las aplicaciones y de los usuarios en las máquinas virtuales.

La instancia de Storage APIs - Data Protection que ofrece VMware funciona con productos de terceros. Cuando utiliza las API, el software de terceros puede realizar copias de seguridad sin cargar los hosts ESXi con el procesamiento de tareas de copia de seguridad.

Los productos de terceros que utilizan Storage APIs - Data Protection pueden realizar las tareas de copia de seguridad siguientes:

- Realizar una copia de seguridad de imagen incremental, diferencial y completa, y restaurar las máquinas virtuales.
- Realizar una copia de seguridad en el nivel de los archivos de las máquinas virtuales que utilizan sistemas operativos Windows y Linux compatibles.
- Garantizar la consistencia de los datos con servicios de snapshots de volumen (VSS) de Microsoft para máquinas virtuales que ejecutan sistemas operativos Microsoft Windows.

Debido a que Storage APIs - Data Protection usa las capacidades de instantánea de VMFS, las copias de seguridad no requieren que se detengan las máquinas virtuales. Estas copias de seguridad se realizan sin interrupciones, pueden llevarse a cabo en cualquier momento y no necesitan ventanas de copia de seguridad extendidas.

Para obtener información sobre Storage APIs - Data Protection y la integración con los productos de copia de seguridad, consulte el sitio web de VMware o póngase en contacto con su proveedor.

Usar ESXi con SAN de canal de fibra

4

Al configurar hosts ESXi para que usen matrices de almacenamiento SAN de canal de fibra, se deben tener en cuenta algunas consideraciones especiales. En esta sección, se incluye información introductoria sobre la forma de usar ESXi con una matriz SAN de canal de fibra.

Este capítulo incluye los siguientes temas:

Conceptos de SAN de canal de fibra

Si es un administrador de ESXi que planifica configurar hosts para que trabajen junto con SAN, debe tener un conocimiento práctico de los conceptos de SAN. Puede encontrar información sobre SAN impresa y en Internet. Debido a que esta industria está en permanente cambio, es conveniente consultar estos recursos con frecuencia.

Si hace poco tiempo que conoce la tecnología SAN, recomendamos que se familiarice con la terminología básica.

Una red de área de almacenamiento (SAN) es una red de alta velocidad especializada que conecta servidores de hosts con subsistemas de almacenamiento de alto rendimiento. Entre los componentes de SAN se encuentran adaptadores de bus de host (HBA) en los servidores del host, conmutadores que ayudan a enrutar el tráfico de almacenamiento, cables, procesadores de almacenamiento (SP) y matrices de discos de almacenamiento.

Una topología SAN con al menos un conmutador presente en la red forma un tejido SAN.

Para transferir tráfico de los servidores de host al almacenamiento compartido, la SAN utiliza el protocolo de canal de fibra (FC), que empaqueta comandos SCSI en tramas de canal de fibra.

Para restringir el acceso del servidor a las matrices de almacenamiento no asignadas a ese servidor, la SAN utiliza la división en zonas. Por lo general, se crean zonas para cada grupo de servidores que accede a un grupo compartido de dispositivos de almacenamiento y LUN. Las zonas definen cuáles HBA pueden conectarse a cuáles SP. Los dispositivos fuera de una zona no son visibles para los dispositivos incluidos en ella.

La división en zonas es similar al enmascaramiento de LUN que, por lo general, se utiliza para la administración de permisos. El enmascaramiento de LUN es un proceso mediante el cual se permite que un LUN esté disponible para ciertos hosts y no lo esté para otros.

Al transferir datos entre el almacenamiento y el servidor del host, la SAN utiliza una técnica denominada múltiples rutas. La función de múltiples rutas permite contar con más de una ruta de acceso física desde el host ESXi hasta el LUN de un sistema de almacenamiento.

Por lo general, una sola ruta de acceso de un host a un LUN está compuesta por un HBA, puertos de conmutación, cables de conexión y el puerto de la controladora de almacenamiento. Si cualquier componente de la ruta de acceso presenta errores, el host selecciona otra ruta disponible para E/S. El proceso de detección de una ruta de acceso con errores se denomina conmutación por error de la ruta de acceso.

Puertos en SAN de canal de fibra

En el contexto de este documento, un puerto es la conexión de un dispositivo a la SAN. Cada nodo de la SAN, como un host, un dispositivo de almacenamiento o un componente del tejido, tiene uno o más puertos que lo conectan a la SAN. Los puertos se identifican de varias formas.

WWPN (World Wide Port Name)

Un identificador único global de un puerto que permite que ciertas aplicaciones accedan al puerto. Los conmutadores de FC detectan el WWPN de un dispositivo o un host y asignan una dirección de puerto al dispositivo.

Port_ID (o dirección de puerto)

Dentro de una SAN, cada puerto tiene un identificador de puerto único que actúa como la dirección de FC del puerto. Este identificador único permite el enrutamiento de datos a través de la SAN a ese puerto. Los conmutadores de FC asignan el identificador de puerto cuando el dispositivo inicia sesión en el tejido. El identificador de puerto es válido solo mientras el dispositivo esté conectado.

Cuando se utiliza la virtualización de identificador de puerto N (NPIV), un único puerto de HBA de FC (N-port) puede registrarse en el tejido con varios WWPN. Este método permite que un puerto N reclame varias direcciones de tejido, cada una de las cuales aparece como una entidad única. Cuando los hosts ESXi utilizan una SAN, estos identificadores varios y únicos permiten la asignación de WWN a máquinas virtuales individuales como parte de la configuración.

Tipos de matrices de almacenamiento de canal de fibra

ESXi admite distintas matrices y sistemas de almacenamiento.

Entre los tipos de almacenamiento que admite un host se encuentran activo-activo, activo-pasivo y compatible con ALUA.

Sistema de almacenamiento activo-activo

Permite acceder simultáneamente a los LUN en todos los puertos de almacenamiento que están disponibles sin una degradación significativa del rendimiento. Todas las rutas de acceso están activas, a menos que se produce un error en alguna de ellas.

Sistema de almacenamiento activo-pasivo

Un sistema en el cual un procesador de almacenamiento proporciona acceso de forma activa a un LUN determinado. Los otros procesadores actúan como copia de seguridad del LUN y pueden proporcionar acceso activamente a otras operaciones de E/S del LUN. Las operaciones de E/S pueden enviarse correctamente solo a un puerto activo de un LUN determinado. Si el acceso a través del puerto de almacenamiento activo genera errores, uno de los procesadores de almacenamiento pasivos puede activarse mediante los servidores que acceden a él.

Sistema de almacenamiento asimétrico

Admite acceso asimétrico a unidades lógicas (ALUA). Los sistemas de almacenamiento compatibles con ALUA ofrecen diferentes niveles de acceso por puerto. Con ALUA, el host puede determinar los estados de los puertos de destino y priorizar las rutas de acceso. El host utiliza algunas de las rutas de acceso activas como principales y otras como secundarias.

Usar la división en zonas con las SAN de canal de fibra

La división en zonas proporciona control de acceso en la topología de la SAN. La división en zonas define qué HBA pueden conectarse a cuáles destinos. Cuando configura una SAN con la división en zonas, los dispositivos fuera de una zona no son visibles para los dispositivos dentro de la zona.

La división en zonas tiene los efectos siguientes:

- Disminuye la cantidad de destinos y LUN que se presentan a un host.
- Controla y aísla las rutas en un tejido.
- Puede evitar que otros sistemas que no sean ESXi accedan a un sistema de almacenamiento en especial y que, posiblemente, destruyan los datos de VMFS.
- Se puede usar para separar distintos entornos, por ejemplo, uno de prueba de uno de producción.

Con hosts ESXi, use una división en zonas de un solo iniciador o una división en zonas de un solo destino y un solo iniciador. La última opción es una de las divisiones en zonas preferidas. El uso de una división en zonas más restrictiva evita problemas y errores de configuración que pueden suceder en la SAN.

Para obtener instrucciones detalladas y las mejores prácticas de la división en zonas, póngase en contacto con los proveedores del conmutador o de las matrices de almacenamiento.

Cómo acceden las máquinas virtuales a los datos en una SAN de canal de fibra

ESXi almacena los archivos del disco de una máquina virtual en un almacén de datos de VMFS que reside en un dispositivo de almacenamiento SAN. Cuando los sistemas operativos invitados de la máquina virtual emiten comandos SCSI a sus discos virtuales, la capa de virtualización SCSI traduce esos comandos a operaciones de archivos VMFS.

Cuando una máquina virtual interactúa con su disco virtual almacenado en una SAN, se llevan a cabo los siguientes procesos:

1. Cuando el sistema operativo invitado de una máquina virtual lee o escribe en el disco SCSI, emite comandos SCSI al disco virtual.
2. Los controladores de dispositivos en el sistema operativo de la máquina virtual se comunican con las controladoras SCSI virtuales.
3. La controladora SCSI virtual reenvía el comando al VMkernel.
4. El VMkernel realiza las siguientes tareas.
   a. Busca el archivo de disco virtual apropiado en el volumen VMFS.
   b. Asigna las solicitudes de los bloques en el disco virtual en bloques del dispositivo físico apropiado.
   c. Envía la solicitud de E/S modificada del controlador del dispositivo en el VMkernel al HBA físico.
5. El HBA físico realiza las siguientes tareas.
   a. Empaqueta la solicitud de E/S según las reglas del protocolo de FC.
   b. Transmite la solicitud a la SAN.
6. En función del puerto que HBA utilice para conectarse al tejido, uno de los conmutadores de SAN recibirá la solicitud. El conmutador dirigirá la solicitud al dispositivo de almacenamiento que corresponda.

Configurar almacenamiento de canal de fibra

5

Cuando se utilizan sistemas ESXi con almacenamiento SAN, existen requisitos de hardware y de sistema específicos.

Este capítulo incluye los siguientes temas:

ESXi Requisitos del SAN de canal de fibra

Como preparación para configurar la SAN y el sistema ESXi para que utilice almacenamiento SAN, repase los requisitos y las recomendaciones.

- Asegúrese de que los sistemas ESXi admiten las combinaciones hardware y firmware de almacenamiento SAN que utiliza. Para acceder a una lista actualizada, consulte la *Guía de compatibilidad de VMware*.
- Configure el sistema para que tenga un solo volumen VMFS por LUN.
- A menos que esté utilizando servidores sin discos, no configure la partición de diagnóstico en un LUN de SAN.

  Si utiliza servidores sin discos que arranquen desde una SAN, es apropiado usar una partición de diagnóstico compartida.
- Use RDM para acceder a discos sin formato. Para obtener información, consulte Capítulo 19 Asignación de dispositivos sin formato.
- Para que la funcionalidad de múltiples rutas funcione adecuadamente, cada LUN debe presentar el mismo número de identificador de LUN para todos los hosts ESXi.
- Asegúrese de que el controlador del dispositivo de almacenamiento especifique una cola lo suficientemente extensa. Puede establecer la profundidad de la cola del HBA físico durante la configuración del sistema.

- En máquinas virtuales que ejecutan Microsoft Windows, aumente el valor del parámetro de SCSI `TimeoutValue` a 60. Con este aumento, Windows puede tolerar retrasos en E/S provocados por una conmutación por error de la ruta de acceso. Para obtener información, consulte Establecer el tiempo de espera en un sistema operativo invitado Windows.

Restricciones de SAN de canal de fibra de ESXi

Cuando se utiliza ESXi con una SAN, aplican ciertas restricciones.

- ESXi no es compatible con dispositivos de cinta conectados a FC.
- No se puede utilizar software de múltiples rutas dentro de una máquina virtual para realizar el equilibrio de carga de E/S de un único LUN físico. Sin embargo, cuando la máquina virtual de Microsoft Windows utiliza discos dinámicos, esta restricción no aplica. Para obtener información sobre la configuración de discos dinámicos, consulte Configurar reflejo de discos dinámico.

Establecer asignaciones de LUN

En este tema, se proporciona información general sobre cómo asignar LUN cuando ESXi trabaja con SAN.

Cuando configura asignaciones de LUN, tenga en cuenta lo siguiente:

Aprovisionamiento de almacenamiento

Para garantizar que el sistema ESXi reconozca los LUN en el momento del inicio, aprovisione todos los LUN en los HBA adecuados antes de conectar la SAN al sistema ESXi.

Aprovisione todos los LUN a todos los HBA ESXi al mismo tiempo. La conmutación por error de HBA funciona solo si todos los HBA ven los mismos LUN.

En el caso de los LUN que se comparten entre varios hosts, asegúrese de que los identificadores de LUN sean coherentes en todos los hosts.

vMotion y DRS de VMware

Cuando usa vCenter Server y vMotion o DRS, asegúrese de que los LUN de las máquinas virtuales se aprovisionen en todos los hosts ESXi. Esta acción proporciona la mayor capacidad para mover máquinas virtuales.

Matrices activa-activa en comparación con activa-pasiva

Cuando use vMotion o DRS con un dispositivo de almacenamiento SAN activo-pasivo, asegúrese de que todos los sistemas ESXi tengan rutas de acceso coherentes con todos procesadores de almacenamiento. Si no lo hace, puede provocar la destrucción de las rutas de acceso cuando se produzca una migración de vMotion.

En el caso de las matrices de almacenamiento activo-pasivo que no figuran en Compatibilidad con almacenamiento/SAN, VMware no admite la conmutación por error de puerto de almacenamiento. En esos casos, debe conectar el servidor al puerto activo en la matriz de almacenamiento. Esta configuración garantiza que los LUN se presenten al host ESXi.

Establecer los HBA de canal de fibra

Por lo general, los HBA de canal de fibra que se utilizan en el host ESXi funcionan correctamente con las opciones de configuración predeterminadas.

Debe seguir las instrucciones de configuración proporcionadas por el proveedor de la matriz de almacenamiento. Durante la configuración del HBA de canal de fibra, tenga en cuenta lo siguiente.

- No combine HBA de canal de fibra de diferentes proveedores en un solo host. Se admiten diferentes modelos del mismo HBA, pero no se puede acceder a un solo LUN con dos tipos de HBA diferentes; eso solo es posible a través del mismo tipo de HBA.
- Asegúrese de que el nivel de firmware en cada HBA sea el mismo.
- Establezca el valor de tiempo de espera para detectar la conmutación por error. Para garantizar un rendimiento óptimo, no cambie el valor predeterminado.
- ESXi admite 32 Gbps de conectividad de canal de fibra de extremo a extremo.

Pasos de instalación y configuración

En este tema se ofrece una descripción general de los pasos de instalación y configuración que se deben seguir al configurar el entorno de SAN para que funcione con ESXi.

Siga estos pasos para configurar el entorno de SAN de ESXi.

1. Si aún no está configurada, debe diseñar la SAN. La mayoría de las SAN existentes requieren solo modificaciones menores para funcionar con ESXi.
2. Compruebe que todos los componentes de la SAN cumplan con los requisitos.
3. Realice todas las modificaciones necesarias en la matriz de almacenamiento.

   La mayoría de los proveedores poseen documentación específica para configurar una SAN de modo que funcione junto con VMware ESXi.
4. Configure los HBA para los hosts que conectó a la SAN.
5. Instale ESXi en los hosts.
6. Cree máquinas virtuales e instale sistemas operativos invitados.
7. (Opcional) Configure el sistema para la conmutación por error de VMware HA o para utilizar Microsoft Clustering Services.
8. Actualice o modifique el entorno según sea necesario.

Virtualizar identificador de puerto N

La virtualización de identificador de puerto N (NPIV) es un estándar ANSI T11 que describe cómo un puerto HBA de canal de fibra único puede registrarse con el tejido usando varios nombres

de puertos universales (WWPN). Esto permite que un puerto N ligado a un tejido reclame varias direcciones de tejido. Cada dirección aparece como entidad única en el tejido de canal de fibra.

Funcionamiento del acceso al LUN basado en NPIV

NPIV permite que un solo puerto HBA de FC registre varios identificadores World Wide Name (WWN) únicos en el tejido, y cada uno de ellos puede asignarse a una máquina virtual individual. Al utilizar NPIV, el administrador de SAN puede supervisar y enrutar el acceso de almacenamiento por una máquina virtual.

Solo las máquinas virtuales con RDM pueden tener asignaciones de WWN, que usan para todo el tráfico RDM.

Cuando una máquina virtual tiene un WWN asignado, el archivo de configuración de la máquina virtual (.vmx) se actualiza para incluir un par de WWN. El par de WWN consta de un WWPN (World Wide Port Name) y un WWNN (World Wide Node Name). Cuando se enciende esa máquina virtual, el VMkernel crea un puerto virtual (Virtual Port, VPORT) en el HBA físico que se utiliza para acceder al LUN. El VPORT es un HBA virtual que aparece en el tejido de canal de fibra como un HBA físico. Como su identificador único, el VPORT usa el par WWN que se asignó a la máquina virtual.

Cada VPORT es específico de la máquina virtual. El VPORT se destruye en el host y ya no aparece en el tejido de FC cuando se apaga la máquina virtual. Cuando se migra una máquina virtual de un host a otro, el VPORT se cierra en el primer host y se abre en el host de destino.

Cuando las máquinas virtuales no tienen asignaciones de WWN, acceden a los LUN de almacenamiento con los WWN de los HBA físicos del host.

Requisitos para utilizar NPIV

Si planea habilitar NPIV en las máquinas virtuales, debe conocer ciertos requisitos.

- NPIV puede usarse solo con las máquinas virtuales que tienen RDM. Las máquinas virtuales que tienen discos virtuales normales usan los WWN de los HBA físicos del host.
- Los HBA del host deben ser compatibles con NPIV.

  Para obtener información, consulte la *Guía de compatibilidad de VMware* y la documentación del proveedor.

  - Use HBA del mismo tipo. VMware no admite que HBA heterogéneos en el mismo host accedan a los mismos LUN.
  - Si un host usa varios HBA físicos como rutas al almacenamiento, divida en zonas todas las rutas físicas a la máquina virtual. Esto es necesario para admitir múltiples rutas, a pesar de que solo habrá una ruta de acceso activa a la vez.
  - Asegúrese de que los HBA físicos en el host puedan detectar todos los LUN a los que deben acceder las máquinas virtuales habilitadas para NPIV que se ejecutan en ese host.
- Los conmutadores en el tejido deben tener reconocimiento de NPIV.

- Cuando configure un LUN para el acceso de NPIV en el nivel del almacenamiento, asegúrese de que el número LUN de NPIV y el identificador de destino de NPIV coincidan con el LUN y el identificadores de destino físicos.
- Divida en zonas los WWPN de NPIV para que se conecten a todos los sistemas de almacenamiento a los que pueden acceder los hosts del clúster, incluso si la máquina virtual no utiliza el almacenamiento. Si agrega sistemas de almacenamiento nuevos a un clúster con una o varias máquinas virtuales habilitadas para NPIV, agregue zonas nuevas de modo que los WWPN de NPIV puedan detectar los puertos de destino de los sistemas de almacenamiento nuevos.

Funcionalidades y limitaciones de NPIV

Obtenga información sobre las capacidades y las limitaciones de la utilización de NPIV con ESXi.

ESXi con NPIV es compatible con:

- NPIV es compatible con vMotion. Cuando se utiliza vMotion para migrar una máquina virtual, se retiene el WWN asignado.

  Si migra una máquina virtual basada en NPIV a un host que no es compatible con NPIV, el VMkernel vuelve a utilizar un HBA físico para enrutar las operaciones de E/S.
- Si el entorno de SAN de canal de fibra admite E/S simultáneas en los discos de una matriz activa-activa, también se admiten operaciones de E/S simultáneas en dos puertos de NPIV diferentes.

Cuando se utiliza ESXi con NPIV, se aplican las siguientes limitaciones:

- Debido a que la tecnología NPIV es una extensión del protocolo de FC, requiere un conmutador de canal de fibra y no funciona en los discos de canal de fibra de conexión directa.
- Cuando se clonan una máquina virtual o una plantilla con un WWN asignado, los clones no retienen el WWN.
- NPIV no es compatible con Storage vMotion.
- Deshabilitar y volver a habilitar la funcionalidad de NPIV en un conmutador de canal de fibra con máquinas virtuales en ejecución puede provocar errores en un vínculo de canal de fibra y la interrupción de las operaciones de E/S.

Configurar o modificar asignaciones de WWN

Asigne la configuración de WWN a la máquina virtual. Más adelante, puede modificar las asignaciones de WWN.

Puede crear entre 1 y 16 pares de WWN, que pueden asignarse a los primeros 1 a 16 HBA de FC físicos en el host.

En general, no es necesario cambiar las asignaciones de WWN existentes en la máquina virtual. En determinadas circunstancias, por ejemplo, cuando los WWN asignados manualmente provocan conflictos en la SAN, es posible que deba cambiar o quitar los WWN.

Requisitos previos

- Antes de configurar WWN, asegúrese de que el host ESXi tenga acceso a la lista de control de acceso (Access Control List, ACL) de LUN de almacenamiento configurada en el lado de la matriz.
- Si desea editar WWN existentes, desconecte la máquina virtual.

Procedimiento

1 Haga clic con el botón derecho en una máquina virtual desde el inventario y seleccione **Editar configuración**.

2 Haga clic en la pestaña **Opciones de máquina virtual** y expanda la opción **Canal de fibra NPIV**.

3 Para crear o editar las asignaciones de WWN, seleccione una de las siguientes opciones:

Opción	Descripción
Deshabilitar NPIV temporalmente para esta máquina virtual	Se deshabilita, pero no se eliminan las asignaciones de WWN existentes de la máquina virtual.
Dejar sin modificaciones	Se conservan las asignaciones de WWN existentes. La sección de solo lectura Asignaciones de WWN muestra los valores de puerto y nodo de las asignaciones de WWN existentes.
Generar nuevos WWN	Se generan nuevos WWN y se anulan los WWN existentes. Los WWN de HBA no se ven afectados. Especifique la cantidad de WWNN y WWPN. Se necesita un mínimo de dos WWPN para admitir la conmutación por error con NPIV. Por lo general, se crea solo un WWNN para cada máquina virtual.
Quitar la asignación de WWN	Se eliminan los WWN asignados a la máquina virtual. La máquina virtual utiliza los WWN de HBA para acceder al LUN de almacenamiento.

4 Haga clic en **Aceptar** para guardar los cambios.

Pasos siguientes

Registre los WWN que se han creado recientemente en el tejido.

Configurar el canal de fibra en Ethernet

6

Para acceder al almacenamiento de canal de fibra, un host ESXi puede utilizar el protocolo de canal de fibra en Ethernet (FCoE).

Nota A partir de vSphere 7.0, VMware deja de ser compatible con FCoE de software en entornos de producción.

El protocolo FCoE encapsula las tramas de canal de fibra en tramas Ethernet. Como resultado, el host no necesitará vínculos de canal de fibra especiales para conectarse al almacenamiento de canal de fibra. El host podrá utilizar Ethernet sin pérdida de 10 Gbit para entregar el tráfico de canal de fibra.

Este capítulo incluye los siguientes temas:

Adaptadores de canal de fibra en Ethernet

Para usar canal de fibra en Ethernet (FCoE), configure los adaptadores adecuados en el host.

Los adaptadores que VMware admite generalmente corresponden a dos categorías, adaptadores de FCoE de hardware y adaptadores de FCoE de software que usan la pila de FCoE nativa en ESXi.

Para obtener información sobre los adaptadores que pueden utilizarse con FCoE de VMware, consulte la *Guía de compatibilidad de VMware*

Adaptadores de FCoE de hardware

Esta categoría incluye adaptadores de red convergentes (CNA) especializados y descargados que contienen funcionalidades de red y canal de fibra en la misma tarjeta.

Cuando se instala este tipo de adaptadores, el host detecta y puede usar ambos componentes del CNA. En vSphere Client, el componente de redes aparece como un adaptador de red estándar (vmnic) y el componente de canal de fibra aparece como un adaptador de FCoE (vmhba). No es necesario que configure el adaptador de FCoE de hardware para usarlo.

Adaptadores de FCoE de software

Nota A partir de vSphere 7.0, VMware deja de ser compatible con FCoE de software en entornos de producción.

Un adaptador de FCoE de software usa la pila del protocolo de FCoE nativa en ESXi para realizar parte del procesamiento de FCoE. Debe utilizar el adaptador de FCoE de software con una NIC compatible.

VMware admite dos categorías de NIC con los adaptadores de FCoE de software.

NIC con descarga de FCoE parcial

Es posible que el alcance de las capacidades de descarga dependa del tipo de NIC. Por lo general, las NIC ofrecen protocolo de puente de centro de datos (DCB) y capacidades de descarga de E/S.

NIC sin descarga de FCoE

Cualquier NIC que ofrece el protocolo DCB y tiene una velocidad mínima de 10 Gbps. Los adaptadores de red no se requieren para admitir las capacidades de descarga FCoE.

A diferencia del adaptador de FCoE de hardware, se debe activar el adaptador de software. Antes de activar el adaptador, debe configurar correctamente las redes.

Nota La cantidad de adaptadores de FCoE de software que activa corresponden a la cantidad de puertos de NIC físicos. ESXi admite un máximo de cuatro adaptadores de FCoE de software en un host.

Instrucciones de configuración para FCoE de software

Al configurar el entorno de red para que funcione con FCoE de software de ESXi, siga las instrucciones y las prácticas recomendadas que ofrece VMware.

Instrucciones para conmutadores de red

Nota A partir de vSphere 7.0, VMware deja de ser compatible con FCoE de software en entornos de producción.

Siga estas instrucciones al configurar un conmutador de red para el entorno de FCoE de software:

- En los puertos que se comunican con el host ESXi, deshabilite el protocolo de árbol de expansión (Spanning Tree Protocol, STP). Habilitar el STP puede retrasar la respuesta del protocolo de inicialización (FCoE Initialization Protocol, FIP) en el conmutador y provocar una condición en la que todas las rutas de acceso quedan inactivas (All Paths Down, APD).

  FIP es un protocolo que usa FCoE para detectar e inicializar entidades FCoE en Ethernet.
- Active el control de flujo basado en prioridades (Priority-based Flow Control, PFC) y establézcalo en Automático.
- Asegúrese de tener una versión de firmware compatible en el conmutador FCoE.
- Establezca el valor de MTU de vSwitch en 2.500 o más.

Directrices y prácticas recomendadas para el adaptador de red

Si planea habilitar los adaptadores FCoE de software para que funcionen con adaptadores de red, debe tener en cuenta algunas consideraciones especiales.

- Ya sea que utilice una NIC parcialmente descargada o una NIC no compatible con FCoE, asegúrese de tener el microcódigo más reciente instalado en el adaptador de red.
- Si utiliza una NIC no compatible con FCoE, asegúrese de que la tarjeta tenga la capacidad DCB para la habilitación de FCoE de software.
- Al configurar las redes, debe agregar cada puerto a un conmutador virtual distinto si el adaptador de red tiene varios puertos. Esta práctica ayuda a evitar una condición APD en caso de que se produzca un evento disruptivo, como un cambio de MTU.
- No mueva un puerto de adaptador de red de un conmutador virtual a otro cuando hay tráfico FCoE activo. Si realiza este cambio, reinicie el host posteriormente.
- Si cambió el conmutador virtual por un puerto de adaptador de red y provocó un error, vuelva a colocar el puerto en el conmutador virtual original para resolver el problema.

Configurar redes para FCoE de software

Antes de activar los adaptadores de FCoE de software en el host ESXi, cree adaptadores de red VMkernel para todas las NIC físicas de FCoE instaladas en el host.

Nota A partir de vSphere 7.0, VMware deja de ser compatible con FCoE de software en entornos de producción.

Este procedimiento explica cómo crear un solo adaptador de red VMkernel conectado a un solo adaptador de red físico FCoE a través de un conmutador de vSphere Standard. Si el host tiene varios adaptadores de red o varios puertos en el adaptador, conecte cada NIC de FCoE a un conmutador estándar distinto. Para obtener más información, consulte la documentación sobre *Redes de vSphere*.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.
2 Haga clic en **Acciones > Agregar redes**.
3 Seleccione **Adaptador de red de VMkernel** y haga clic en **Siguiente**.
4 Seleccione **Nuevo conmutador estándar** para crear un conmutador de vSphere Standard.
5 Para habilitar las tramas gigantes, cambie la **MTU (Bytes)** al valor de 2.500 o más y haga clic en **Siguiente**.
6 Haga clic en el icono **Agregar adaptadores** y seleccione el adaptador de red (vmnic#) compatible con FCoE.

   Asegúrese de asignar el adaptador a Adaptadores activos.
7 Introduzca una etiqueta de red.

   La etiqueta de red es un nombre simple que identifica el adaptador de VMkernel que se está creando, por ejemplo, FCoE.
8 Especifique un identificador de VLAN y haga clic en **Siguiente**.

   El tráfico de FCoE requiere una red aislada. Asegúrese de que el identificador de VLAN que especifique sea diferente del que usó para el tráfico de redes común en el host. Para obtener más información, consulte la documentación sobre *Redes de vSphere*.
9 Después de terminar la configuración, revise la información y haga clic en **Finalizar**.

Resultados

Creó el adaptador de VMkernel virtual para el adaptador de red de FCoE físico instalado en el host.

Nota Para evitar interrupciones en el tráfico de FCoE, no quite el adaptador de red de FCoE (vmnic#) del conmutador de vSphere Standard después de configurar las redes de FCoE.

Agregar adaptadores de FCoE de software

Es necesario activar los adaptadores de FCoE de software para que el host ESXi pueda utilizarlos para acceder al almacenamiento de canal de fibra.

Nota A partir de vSphere 7.0, VMware deja de ser compatible con FCoE de software en entornos de producción.

La cantidad de adaptadores de FCoE de software que se puede activar corresponde a la cantidad de puertos de NIC de FCoE físicos en el host. ESXi admite un máximo de cuatro adaptadores de FCoE de software en un host.

Requisitos previos

Configure las redes del adaptador de FCoE de software.

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y, a continuación, en el icono **Agregar adaptador de software**.
4. Seleccione **Adaptador de FCoE de software**.
5. En el cuadro de diálogo Agregar adaptador de FCoE de software, seleccione una vmnic en la lista desplegable de adaptadores de red físicos.

   Solo aparecen los adaptadores que aún no se utilizan para el tráfico de FCoE.
6. Haga clic en **Aceptar**.

   El adaptador de FCoE de software aparece en la lista de adaptadores de almacenamiento.

Resultados

Una vez activado el adaptador de FCoE de software, es posible ver sus propiedades. Si no utiliza el adaptador, puede eliminarlo de la lista de adaptadores.

Arrancar ESXi desde una SAN de canal de fibra

7

Cuando se configura el host para arrancar desde una SAN, la imagen de arranque del host se almacena en uno o más LUN en el sistema de almacenamiento SAN. Cuando el host arranca, lo hace desde el LUN en la SAN, no desde su disco local.

ESXi admite el arranque a través de un adaptador de bus host (HBA) de canal de fibra o un adaptador de red convergente (CNA) de canal de fibra en Ethernet (FCoE).

Este capítulo incluye los siguientes temas:

Beneficios del arranque desde SAN

El arranque desde SAN puede ofrecer numerosos beneficios para el entorno de ESXi. Sin embargo, en ciertos casos, el arranque desde una SAN no es compatible con los hosts. Antes de configurar el sistema para el arranque desde SAN, decida si es apropiado para el entorno.

Precaución Cuando utiliza el arranque desde SAN con varios hosts ESXi, cada host debe tener su propio LUN de arranque. Si configura varios hosts para que compartan el LUN de arranque, es probable que se produzcan daños en la imagen de ESXi.

Si utiliza el arranque desde SAN, estas son algunas de las ventajas de las que se beneficiará el entorno:

- Servidores más económicos. Los servidores pueden ser más densos y funcionar con menos temperatura sin almacenamiento interno.
- Reemplazo más sencillo de los servidores. Cuando reemplaza servidores, el nuevo servidor puede apuntar a la ubicación de arranque anterior.
- Menos espacio desperdiciado. Con frecuencia, los servidores sin discos locales ocupan menos espacio.

- Procesos más sencillos de copia de seguridad. Puede realizar copias de seguridad de imágenes de arranque del sistema en la SAN como parte de los procedimientos generales de copia de seguridad de la SAN. Además, puede utilizar características avanzadas de la matriz, como snapshots en la imagen de arranque.
- Administración mejorada. Crear y administrar la imagen del sistema operativo es más sencillo y eficiente.
- Mayor confiabilidad. Puede acceder al disco de arranque a través de múltiples rutas, lo que protege al disco y evita que sea un único punto de error.

Requisitos y consideraciones al arrancar desde SAN de canal de fibra

La configuración de arranque de ESXi debe cumplir requisitos específicos.

Tabla 7-1. Requisitos para arranque desde SAN

Requisito	Descripción
Requisitos del sistema ESXi	Siga las recomendaciones del proveedor sobre el arranque del servidor desde una SAN.
Requisitos del adaptador	Configure el adaptador para que pueda acceder al LUN de arranque. Consulte la documentación del proveedor.
Control de acceso	■ Cada host debe tener acceso solo a su propio LUN de arranque, no a los LUN de arranque de otros hosts. Utilice el software del sistema de almacenamiento para asegurarse de que el host acceda solo a los LUN designados. ■ Varios servidores pueden compartir una partición de diagnóstico. Para lograr esta configuración puede utilizar el enmascaramiento de LUN específico para matrices.
Compatibilidad con múltiples rutas	No se pueden habilitar múltiples rutas para un LUN de arranque en matrices activas-pasivas porque el BIOS no admite múltiples rutas y no puede activar una ruta de acceso en espera.
Consideraciones sobre SAN	Si la matriz no está certificada para una topología de conexión directa, las conexiones de SAN deben realizarse a través de una topología conmutada. Si la matriz está certificada para la topología de conexión directa, las conexiones de SAN pueden realizarse directamente a esa matriz. El arranque desde SAN es compatible con ambas topologías: la de conexión directa y la conmutada.
Consideraciones específicas sobre hardware	Si ejecuta un IBM eServer BladeCenter y utiliza el arranque desde una SAN, debe deshabilitar las unidades IDE en los blades.

Prepararse para el arranque desde SAN

Cuando se prepara el host ESXi para arrancar desde una SAN, se realizan varias tareas.

Esta sección describe el proceso de habilitación genérico de arranque desde SAN en los servidores montados en bastidores. Para obtener información sobre cómo habilitar el arranque desde la opción de SAN en servidores blade FCoE Cisco Unified Computing System, consulte la documentación de Cisco.

Procedimiento

1 Configurar los componentes de la SAN y del sistema de almacenamiento

   Antes de configurar el host ESXi para arrancar desde un LUN de SAN, configure los componentes de la SAN y un sistema de almacenamiento.

2 Configurar adaptador de almacenamiento para arrancar desde SAN

   Cuando el host se configura para arrancar desde la SAN, se habilita el adaptador de arranque en el BIOS del host. A continuación, se debe configurar el adaptador de arranque para que inicie una conexión primitiva con el LUN de arranque de destino.

3 Configurar sistema para arrancar desde los medios de instalación

   Al configurar el host para arrancar desde SAN, primero se debe arrancar el host desde el medio de instalación de VMware. Para arrancar desde los medios de instalación, cambie la secuencia de arranque del sistema en la configuración del BIOS.

Configurar los componentes de la SAN y del sistema de almacenamiento

Antes de configurar el host ESXi para arrancar desde un LUN de SAN, configure los componentes de la SAN y un sistema de almacenamiento.

Debido a que la configuración de componentes de SAN es específica del proveedor, debe consultar la documentación del producto para cada elemento.

Procedimiento

1 Conecte el cable de red, consultando cualquier guía de cableado que se aplique a la instalación.

   Revise el cableado del conmutador, si lo hubiera.

2 Configure la matriz de almacenamiento.

   a Desde la matriz de almacenamiento SAN, haga que el host ESXi sea visible para la SAN. A menudo, este proceso se denomina creación de un objeto.

   b Desde la matriz de almacenamiento SAN, configure el host para que tenga los WWPN de los adaptadores del host como nombres de puerto o nombres de nodo.

   c Cree los LUN.

   d Asigne los LUN.

e Registre las direcciones IP de los conmutadores y las matrices de almacenamiento.

f Registre el WWPN de cada SP.

Precaución Si utiliza un proceso de instalación generado por script para que ESXi arranque en modo de SAN, siga los pasos especiales para que no se pierdan datos.

Configurar adaptador de almacenamiento para arrancar desde SAN

Cuando el host se configura para arrancar desde la SAN, se habilita el adaptador de arranque en el BIOS del host. A continuación, se debe configurar el adaptador de arranque para que inicie una conexión primitiva con el LUN de arranque de destino.

Requisitos previos

Determine el WWPN para el adaptador de almacenamiento.

Procedimiento

- Configure el adaptador de almacenamiento para que arranque desde la SAN.

  Debido a que la configuración de los adaptadores de arranque depende del proveedor, es necesario consultar la documentación del proveedor.

Configurar sistema para arrancar desde los medios de instalación

Al configurar el host para arrancar desde SAN, primero se debe arrancar el host desde el medio de instalación de VMware. Para arrancar desde los medios de instalación, cambie la secuencia de arranque del sistema en la configuración del BIOS.

Debido a que el procedimiento de cambio de la secuencia de arranque en el BIOS es específico de cada proveedor, consulte la documentación del proveedor para obtener instrucciones. A continuación, se explica cómo cambiar la secuencia de arranque en un host de IBM.

Procedimiento

1 Encienda el sistema e introduzca la utilidad de configuración del BIOS del sistema.

2 Seleccione **Opciones de inicio** y presione Entrar.

3 Seleccione **Opciones de la secuencia de inicio** y presione Entrar.

4 Cambie la opción **Primer dispositivo de inicio** a **[CD-ROM]**.

Resultados

Ahora ya puede instalar ESXi.

Configurar HBA de Emulex para arrancar desde SAN

La configuración del BIOS del HBA de Emulex para arrancar desde SAN incluye la habilitación del símbolo de BootBIOS y del BIOS.

Procedimiento

1 Habilitar el símbolo de BootBIOS

   Al configurar el BIOS de HBA Emulex para que arranque ESXi desde SAN, se debe habilitar el símbolo de BootBIOS.

2 Habilitar el BIOS

   Cuando configura el BIOS del HBA Emulex para que arranque ESXi desde SAN, debe habilitar el BIOS.

Habilitar el símbolo de BootBIOS

Al configurar el BIOS de HBA Emulex para que arranque ESXi desde SAN, se debe habilitar el símbolo de BootBIOS.

Procedimiento

1 Ejecute `lputil`.

2 Seleccione **3. Firmware Maintenance** (3. Mantenimiento de firmware).

3 Seleccione un adaptador.

4 Seleccione **6. BootBIOS Maintenance** (6. Mantenimiento de BootBIOS).

5 Seleccione **1. Enable BootBIOS** (1. Habilitar BootBIOS).

Habilitar el BIOS

Cuando configura el BIOS del HBA Emulex para que arranque ESXi desde SAN, debe habilitar el BIOS.

Procedimiento

1 Reinicie el host.

2 Para configurar los parámetros del adaptador, presione ALT+E en el símbolo de Emulex y siga estos pasos.

   a Seleccione un adaptador (compatible con BIOS).

   b Seleccione **2. Configurar los parámetros de este adaptador**.

   c Seleccione **1. Habilitar o deshabilitar el BIOS**.

   d Seleccione **1** para habilitar el BIOS.

   e Seleccione **x** para salir y **Esc** para regresar al menú anterior.

3 Para configurar el dispositivo de arranque, siga estos pasos en el menú principal de Emulex.

   a Seleccione el mismo adaptador.

   b Seleccione **1. Configurar dispositivos de arranque**.

   c Seleccione la ubicación de la entrada de arranque.

   d Introduzca el dispositivo de arranque de dos dígitos.

   e Introduzca el LUN de inicio de dos dígitos hexadecimales (por ejemplo, `08`).

   f Seleccione el LUN de arranque.

   g Seleccione **1. WWPN.** Arranque este dispositivo con WWPN, no con DID.

   h Seleccione **x** para salir e **Y** para reiniciar.

4 Arranque en el BIOS del sistema y mueva Emulex al primer lugar en la secuencia de la controladora de arranque.

5 Reinícielo e instálelo en un LUN de SAN.

Configurar HBA de QLogic para arrancar desde SAN

Este procedimiento de muestra explica cómo configurar el HBA QLogic para arrancar ESXi desde SAN. El procedimiento implica habilitar el BIOS del HBA QLogic, habilitar el arranque seleccionable y seleccionar el LUN de arranque.

Procedimiento

1 Mientras arranca el servidor, presione **Ctrl+Q** para entrar a la utilidad de configuración Fast! UTIL.

2 Realice la acción adecuada según la cantidad de HBA.

Opción	Descripción
Un HBA	Si solo tiene un HBA, aparecerá la página Opciones de Fast!UTIL. Salte al Paso 3.
Varios HBA	Si tiene más de un HBA, seleccione el HBA manualmente. a En la página Seleccionar adaptador de host, utilice las teclas de flecha para ubicar el cursor en el HBA adecuado. b Presione **Entrar**.

3 En la página Opciones de Fast!UTIL, seleccione **Opciones de configuración** y presione **Entrar**.

4 En la página Opciones de configuración, seleccione **Configuración del adaptador** y presione **Entrar**.

5 Establezca el BIOS para que busque dispositivos SCSI.

   a En la página Configuración del adaptador de host, seleccione **BIOS del adaptador de host**.

   b Presione **Entrar** para alternar el valor a **Habilitado**.

   c Presione **Esc** para salir.

6 Habilite el arranque seleccionable.

   a Seleccione **Configuración del arranque seleccionable** y presione **Entrar**.

   b En la página Configuración del arranque seleccionable, seleccione **Arranque seleccionable**.

   c Presione **Entrar** para alternar el valor a **Habilitado**.

7 Seleccione la entrada de nombre de puerto de arranque en la lista de procesadores de almacenamiento (SP) y pulse la tecla **Entrar**.

   Se abrirá la página Seleccionar dispositivo de canal de fibra.

8 Seleccione el SP específico y pulse **Entrar**.

   Si va a utilizar una matriz de almacenamiento de tipo activo-pasivo, el SP seleccionado debe estar en la ruta de acceso (activa) preferida al LUN de arranque. Si no está seguro respecto de qué SP está en la ruta de acceso activa, utilice el software de administración de matriz de almacenamiento para encontrarlo. El BIOS crea los identificadores de destino, y estos pueden cambiar con cada reinicio.

9 Realice la acción adecuada según la cantidad de LUN asociados al SP.

Opción	Descripción
Un LUN	Se selecciona el LUN como LUN de arranque. No es necesario entrar en la página Seleccionar LUN.
Varios LUN	Se abrirá la página Seleccionar LUN. Utilice el cursor para seleccionar el LUN de arranque y, a continuación, pulse **Entrar**.

10 Si aparece algún otro procesador de almacenamiento restante en la lista, presione **C** para eliminar los datos.

11 Presione **Esc** dos veces para salir y, a continuación, presione **Entrar** para guardar la configuración.

Arrancar ESXi con FCoE de software

8

ESXi admite el arranque desde adaptadores de red compatibles con FCoE.

Solo las NIC con descarga de FCoE parcial son compatibles con las capacidades de arranque de FCoE de software. Si utiliza las NIC sin descarga de FCoE, no se admite el arranque de FCoE de software.

Cuando se instala y se arranca ESXi desde un LUN de FCoE, el host puede utilizar un adaptador FCoE de software de VMware y un adaptador de red con capacidades de FCoE. El host no requiere un HBA FCoE dedicado.

La mayoría de las configuraciones se realiza a través de la `option ROM` del adaptador de red. Los adaptadores de red deben admitir uno de los formatos siguientes, que comunican parámetros sobre un dispositivo de arranque FCoE al VMkernel.

- Tabla de firmware de arranque de FCoE (FBFT). FBFT es propiedad de Intel.
- Tabla de parámetros de arranque de FCoE (FBPT). VMware define FBPT para que los proveedores de terceros implementen un arranque de FCoE de software.

Los parámetros de configuración se establecen en la `option ROM` del adaptador. Durante la instalación o el arranque posterior de ESXi, estos parámetros se exportan a la memoria del sistema en formato FBFT o FBPT. El VMkernel puede leer las opciones de configuración y utilizarlas para acceder al LUN de arranque.

Este capítulo incluye los siguientes temas:

Requisitos y consideraciones sobre el arranque de FCoE de software

Cuando el host ESXi se arranca desde una SAN con FCoE de software, aplican ciertos requisitos y consideraciones.

Requisitos

- Utilice una versión compatible de ESXi.
- El adaptador de red debe tener las capacidades siguientes:
  - Ser compatible con FCoE.
  - Admitir una pila de FCoE abierta de ESXi.
  - Contener un firmware de arranque de FCoE que pueda exportar información de arranque en formato FBFT o FBPT.

Consideraciones

- No se puede cambiar la configuración de arranque de FCoE de software desde ESXi.
- No se admite el volcado de núcleos en ningún LUN de FCoE de software, incluido el LUN de arranque.
- No se admite la función de múltiples rutas antes del arranque.
- El LUN de arranque no puede compartirse con otros host, incluso en un almacenamiento compartido. Asegúrese de que el host tenga acceso al LUN de arranque completo.

Configurar arranque de FCoE de software

El host ESXi puede arrancar desde un LUN de FCoE con el adaptador FCoE de software y un adaptador de red.

Al configurar el host para una arranque de FCoE de software, debe realizar varias tareas.

Requisitos previos

El adaptador de red tiene las siguientes capacidades:

- Compatibilidad parcial con descargas de FCoE (FCoE de software).
- Contiene una tabla de firmware de arranque de FCoE (FBFT) o una tabla de parámetros de arranque de FCoE (FBPT).

Para obtener información sobre los adaptadores de red compatibles con el arranque de FCoE de software, consulte la *Guía de compatibilidad de VMware*.

Procedimiento

1 Configurar parámetros de arranque de FCoE de software

   Para complementar un proceso de arranque de FCoE de software, un adaptador de red en el host debe tener un firmware de arranque de FCoE especialmente configurado. Al configurar el firmware, habilita el adaptador para el arranque de FCoE de software y especifica los parámetros del LUN de arranque.

2 Instalación y arranque de ESXi desde LUN FCoE de software

Cuando se configura el sistema para que arranque desde un LUN FCoE de software, se instala la imagen de ESXi en el LUN de destino. Posteriormente, es posible arrancar el host desde ese LUN.

Configurar parámetros de arranque de FCoE de software

Para complementar un proceso de arranque de FCoE de software, un adaptador de red en el host debe tener un firmware de arranque de FCoE especialmente configurado. Al configurar el firmware, habilita el adaptador para el arranque de FCoE de software y especifica los parámetros del LUN de arranque.

Procedimiento

◆ En la opción ROM del adaptador de red, especifique los parámetros de arranque de FCoE de software.

Entre estos parámetros se encuentran un destino de arranque, LUN de arranque, identificador de VLAN, etc.

Debido a que la configuración del adaptador de red depende del proveedor, es necesario consultar la documentación del proveedor para obtener instrucciones.

Instalación y arranque de ESXi desde LUN FCoE de software

Cuando se configura el sistema para que arranque desde un LUN FCoE de software, se instala la imagen de ESXi en el LUN de destino. Posteriormente, es posible arrancar el host desde ese LUN.

Requisitos previos

- Configure la `option ROM` para el adaptador de red, de modo que apunte a un LUN de arranque de destino. Asegúrese de tener información acerca del LUN de arranque.
- Cambie el orden de arranque en el BIOS del sistema a la secuencia siguiente:

  a El adaptador de red que utiliza para el arranque de FCoE de software.

  b Los medios de instalación de ESXi.

  Consulte la documentación del proveedor de su sistema.

Procedimiento

1 Inicie una instalación interactiva desde el soporte de instalación de ESXi.

El instalador de ESXi comprueba que el arranque de FCoE esté habilitado en el BIOS y, de ser necesario, crea un conmutador virtual estándar para el adaptador de red compatible con FCoE. El nombre del vSwitch es VMware_FCoE_vSwitch. El instalador utiliza, a continuación, parámetros de arranque de FCoE preconfigurados para detectar y mostrar todos los LUN FCoE disponibles.

2 En la página **Seleccionar un disco**, seleccione el LUN de FCoE de software que especificó en la configuración de parámetros de arranque.

   Si el LUN de arranque no aparece en este menú, asegúrese de haber configurado los parámetros de arranque correctamente en la `option ROM` del adaptador de red.

3 Siga las indicaciones para completar la instalación.

4 Reinicie el host.

5 Cambie el orden de arranque en el BIOS del sistema para que el LUN de arranque de FCoE sea el primer dispositivo de arranque.

   ESXi continúa arrancando desde el LUN FCoE de software hasta que está listo para ser utilizado.

Pasos siguientes

De ser necesario, puede cambiar el nombre y modificar la instancia de VMware_FCoE_vSwitch que creó automáticamente el instalador. Asegúrese de que el modo CDP esté establecido en Escucha o Ambos.

Solución de problemas de arranque de FCoE de software para un host ESXi

Si la instalación o el arranque deESXi desde un LUN de FCoE de software produce errores, puede usar varios métodos de solución de problemas.

Problema

Cuando se instala o arranca ESXi desde el almacenamiento de FCoE, la instalación o el proceso de arranque fallan. La configuración de FCoE que ha utilizado incluye un adaptador de FCoE de software de VMware y un adaptador de red con capacidades de descarga de FCoE parciales.

Solución

- Asegúrese de haber configurado correctamente los parámetros de arranque en la opción ROM del adaptador de red de FCoE.
- Durante la instalación, supervise el BIOS del adaptador de red de FCoE en busca de cualquier error.
- De ser posible, compruebe el registro del VMkernel en busca de errores.
- Use el comando `esxcli` para comprobar que el LUN de arranque esté presente.

  ```
  esxcli conn_options hardware bootdevice list
  ```

Prácticas recomendadas para el almacenamiento de canal de fibra

9

Cuando se utiliza ESXi con SAN de canal de fibra, siga las recomendaciones para evitar problemas de rendimiento.

vSphere Client ofrece varias opciones para recopilar información de rendimiento. La información se muestra de forma gráfica y se actualiza con frecuencia.

También puede usar las utilidades de línea de comandos `resxtop` o `esxtop`. Estas utilidades proporcionan una vista detallada del modo en que ESXi usa los recursos. Para obtener más información, consulte la documentación sobre *Administrar recursos de vSphere*.

Consulte a su representante de almacenamiento si su sistema de almacenamiento admite las características de aceleración de hardware de Storage API - Array Integration. Si las admite, consulte la documentación del proveedor sobre cómo habilitar la compatibilidad con la aceleración de hardware en el sistema de almacenamiento. Para obtener más información, consulte Capítulo 24 Aceleración de hardware de almacenamiento.

Este capítulo incluye los siguientes temas:

Evitar problemas de SAN de canal de fibra

Si usa ESXi junto con una SAN de canal de fibra, siga las instrucciones específicas para evitar problemas en la SAN.

Para evitar problemas con la configuración de SAN, siga estos consejos:

- Coloque un solo almacén de datos de VMFS en cada LUN.
- No cambie la directiva de rutas de acceso que el sistema establece a menos que comprenda las consecuencias de realizar esa modificación.
- Documente todo. Incluya información sobre la división en zonas, el control de acceso, el almacenamiento, el conmutador, el servidor y la configuración del HBA de FC.

- Planificación en caso de errores:
  - Haga varias copias de los mapas de topología. Para cada elemento, tenga en cuenta lo que sucede con la SAN si el elemento presenta errores.
  - Verifique diferentes vínculos, conmutadores, HBA y otros elementos para asegurarse de no haber omitido ningún punto de error crítico en el diseño.
- Asegúrese de que los HBA de canal de fibra estén instalados en las ranuras correctas en el host, según la velocidad del bus y de la ranura. Equilibre la carga del bus PCI entre los buses disponibles del servidor.
- Familiarícese con los distintos puntos de supervisión en la red de almacenamiento, en todos los puntos de visibilidad, incluidos los gráficos de rendimiento, las estadísticas de conmutador de FC y las estadísticas de rendimiento del almacenamiento del host.
- Tenga cuidado cuando cambie los identificadores de los LUN que tienen almacenes de datos de VMFS utilizados por el host ESXi. Si cambia el identificador, el almacén de datos se vuelve inactivo y las máquinas virtuales generan errores. Vuelva a firmar el almacén de datos para activarlo nuevamente. Consulte Administrar almacenes de datos de VMFS duplicados.

  Después de cambiar el identificador del LUN, vuelva a examinar el almacenamiento para restablecer el identificador en el host. Para obtener información sobre cómo volver a examinar, consulte Operaciones para volver a examinar el almacenamiento.

Deshabilitar el registro automático de hosts ESXi

Ciertas matrices de almacenamiento requieren que los hosts ESXi se registren en ellas. ESXi realiza el registro automático de los hosts al enviar el nombre y la dirección IP de los hosts a la matriz. Si prefiere el registro manual mediante el software de administración de almacenamiento, deshabilite la característica de registro automático de ESXi.

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Sistema**, haga clic en **Configuración avanzada del sistema**.
4. En Configuración avanzada del sistema, seleccione el parámetro **Disk.EnableNaviReg** y haga clic en el icono **Editar**.
5. Cambie el valor a 0.

Resultados

Esta operación deshabilita el registro de host automático que está habilitado de manera predeterminada.

Optimizar el rendimiento del almacenamiento de SAN de canal de fibra

Hay varios factores que contribuyen a la optimización del entorno típico de SAN.

Si el entorno está configurado apropiadamente, los componentes del tejido de SAN (particularmente, los conmutadores de la SAN) son solo contribuyentes menores debido a sus latencias bajas relativas en servidores y matrices de almacenamiento. Asegúrese de que las rutas de acceso por el tejido de conmutadores no estén saturadas; es decir, que el tejido de conmutadores funcione con la máxima capacidad de proceso.

Rendimiento de matrices de almacenamiento

El rendimiento de la matriz de almacenamiento es uno de los principales factores que contribuye al rendimiento de todo el entorno SAN.

Si surgen problemas con el rendimiento de la matriz de almacenamiento, consulte la documentación del proveedor de matrices de almacenamiento para buscar toda información que sea relevante.

Si desea mejorar el rendimiento de la matriz en el entorno de vSphere, siga estas instrucciones generales:

- Al asignar LUN, recuerde que varios hosts pueden acceder al LUN, y que es posible ejecutar varias máquinas virtuales en cada host. Un LUN utilizado por un host puede prestar servicios de E/S de varias aplicaciones diferentes ejecutadas en distintos sistemas operativos. Debido a esta carga de trabajo diversa, el grupo RAID que contiene los LUN de ESXi generalmente no incluye LUN utilizados por otros servidores que no ejecuten ESXi.
- Asegúrese de que el almacenamiento en caché de lectura/escritura esté disponible.
- Las matrices de almacenamiento SAN requieren un rediseño y un ajuste continuos para garantizar que la E/S tenga una carga equilibrada en todas las rutas de acceso de las matrices de almacenamiento. Para cumplir con este requisito, distribuya las rutas de acceso a los LUN entre todos los procesadores de almacenamiento (SP). De esa manera, se podrá proporcionar un equilibrio de carga óptimo. Mediante una supervisión minuciosa, se puede determinar cuándo es necesario volver a equilibrar la distribución de LUN.

  El ajuste de matrices de almacenamiento con equilibrio estático es una cuestión de supervisión de las estadísticas de rendimiento específicas, como las operaciones de E/S por segundo, los bloques por segundo y el tiempo de respuesta. También es importante distribuir la carga de trabajo de LUN para propagar la carga de trabajo entre todos los SP.

  Nota El equilibrio de carga dinámico actualmente no es compatible con ESXi.

Rendimiento de servidores con canal de fibra

Se deben tener en cuenta varios factores para garantizar un rendimiento óptimo del servidor.

Cada aplicación del servidor debe tener acceso a su almacenamiento designado con las condiciones siguientes:

- Velocidad de E/S alta (cantidad de operaciones de E/S por segundo)
- Alta capacidad de proceso (megabytes por segundo)
- Latencia mínima (tiempos de respuesta)

Dado que cada aplicación tiene distintos requisitos, puede cumplir estos objetivos eligiendo un grupo RAID adecuado en la matriz de almacenamiento.

Para alcanzar los objetivos de rendimiento, siga estas directrices:

- Coloque cada LUN en un grupo RAID que proporcione los niveles de rendimiento necesarios. Supervise las actividades y el uso de recursos de otros LUN en el grupo RAID asignado.
  Es posible que un grupo RAID de alto rendimiento que tiene demasiadas aplicaciones que realizan operaciones de E/S en él no cumpla con los objetivos de rendimiento requeridos por una aplicación que se ejecuta en el host ESXi.
- Asegúrese de que cada host tenga suficientes HBA para aumentar la capacidad de proceso de las aplicaciones en el host para el período máximo. La propagación de E/S en varios HBA proporciona una capacidad de proceso más rápida y menos latencia para cada aplicación.
- A fin de proporcionar redundancia para un posible error de HBA, asegúrese de que el host esté conectado a un tejido redundante dual.
- Cuando se asignan LUN o grupos RAID a sistemas ESXi, recuerde que varios sistemas operativos usan y comparten ese recurso. El rendimiento de LUN requerido por el host ESXi podría ser mucho mayor que cuando se usan máquinas físicas normales. Por ejemplo, si espera ejecutar cuatro aplicaciones de uso intensivo de E/S, asigne el cuádruple de capacidad de rendimiento al LUN de ESXi.
- Cuando se usan varios sistemas ESXi con vCenter Server, los requisitos de rendimiento para el subsistema de almacenamiento aumentan en consecuencia.
- La cantidad de E/S pendientes requerida por las aplicaciones que se ejecutan en un sistema ESXi debe coincidir con la cantidad de E/S que pueden controlar el HBA y la matriz de almacenamiento.

Usar ESXi con una SAN iSCSI

10

ESXi puede conectarse al almacenamiento SAN externo mediante el protocolo de Internet SCSI (iSCSI). Además de la extensión iSCSI tradicional, ESXi es compatible con las extensiones de iSCSI para RDMA (iSER).

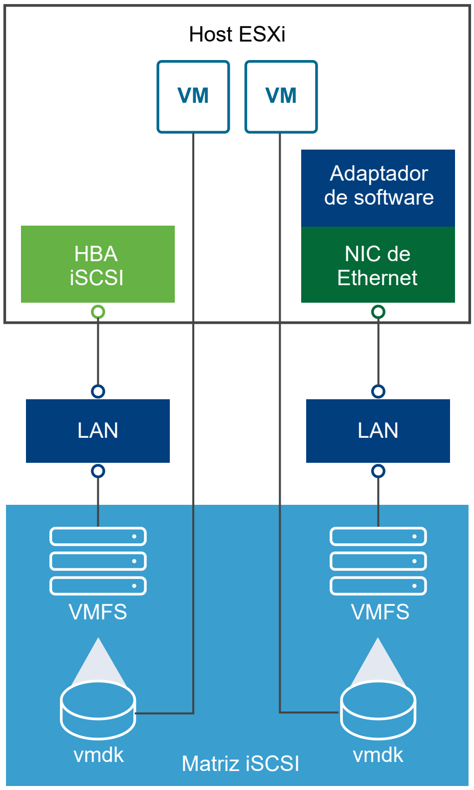
Cuando el protocolo iSER está habilitado, el host puede usar el mismo marco de iSCSI, pero reemplaza el transporte de TCP/IP por el transporte de RDMA.

Este capítulo incluye los siguientes temas:

Acerca de SAN de iSCSI

Las SAN de iSCSI utilizan conexiones Ethernet entre hosts y subsistemas de almacenamiento de alto rendimiento.

En el host, los componentes de SAN de iSCSI incluyen tarjetas de interfaz de red (Network Interface Cards, NIC) o adaptadores de bus de host (Host Bus Adapters, HBA) de iSCSI. La red iSCSI también incluye conmutadores y enrutadores que transfieren tráfico de almacenamiento, cables, procesadores de almacenamiento (Storage Processors, SP) y sistemas de discos de almacenamiento.



La red SAN de iSCSI utiliza una arquitectura de cliente-servidor.

El cliente, denominado iniciador iSCSI, funciona en el host ESXi. Para iniciar las sesiones iSCSI, el iniciador emite comandos de SCSI y los transmite, encapsulados en el protocolo iSCSI, a un servidor iSCSI. El servidor se denomina destino iSCSI. Generalmente, el destino iSCSI representa un sistema de almacenamiento físico en la red.

El destino también puede ser una SAN iSCSI virtual; por ejemplo, un emulador de destinos iSCSI que se ejecute en una máquina virtual. El destino iSCSI responde a los comandos del iniciador transmitiendo los datos iSCSI requeridos.

Múltiples rutas iSCSI

Al transferir datos entre el almacenamiento y el servidor del host, la SAN utiliza una técnica denominada múltiples rutas. Con múltiples rutas, el host ESXi puede tener más de una ruta física a un LUN en un sistema de almacenamiento.

Por lo general, una ruta de acceso individual de un host a un LUN consiste en un adaptador de iSCSI o una NIC, puertos de conmutadores, cables de conexión y el puerto de la controladora de almacenamiento. Si cualquier componente de la ruta de acceso presenta errores, el host selecciona otra ruta disponible para E/S. El proceso de detección de una ruta de acceso con errores se denomina conmutación por error de la ruta de acceso.

Para obtener más información sobre las múltiples rutas, consulte Capítulo 18 Descripción de múltiples rutas y conmutación por error.

Nodos y puertos en SAN de iSCSI

Una entidad detectable individual en la SAN de iSCSI, como un iniciador o un destino, representa un nodo iSCSI.

Cada nodo tiene un nombre de nodo. ESXi utiliza varios métodos para identificar un nodo.

Dirección IP

Cada nodo iSCSI puede tener una dirección IP asociada, de modo que los equipos de enrutamiento y conmutación de la red puedan establecer la conexión entre el host y el almacenamiento. Esta dirección es similar a la dirección IP que se asigna a un equipo para acceder a la red de la empresa o a Internet.

Nombre iSCSI

Un nombre universal único para identificar el nodo. iSCSI utiliza el nombre calificado iSCSI (IQN) y el identificador único extendido (EUI).

De manera predeterminada, ESXi genera nombres iSCSI únicos para los iniciadores iSCSI, por ejemplo, `iqn.1998-01.com.vmware:iscsitestox-68158ef2`. Por lo general, no se debe cambiar el valor predeterminado; caso contrario, el nombre iSCSI nuevo que se introduzca debe ser único.

Alias iSCSI

Un nombre más manejable para un puerto o dispositivo iSCSI que se utiliza en lugar del nombre iSCSI. Los alias iSCSI no son únicos y están diseñados para ser un nombre descriptivo que se puede asociar a un puerto.

Cada nodo tiene uno o varios puertos que lo conectan a la SAN. Los puertos iSCSI son extremos de una sesión iSCSI.

Convenciones de nomenclatura de iSCSI

iSCSI utiliza un nombre único para identificar un nodo de iSCSI, se trate de destino o iniciador.

Los nombres de iSCSI se formatean de dos maneras diferentes. El formato más común es IQN.

Para obtener más detalles sobre los requisitos de nomenclatura y los perfiles de cadenas de iSCSI, consulte RFC 3721 y RFC 3722 en el sitio web de IETF.

Formato de nombre calificado de iSCSI

El formato de nombre calificado (IQN) de iSCSI adopta el formato de `iqn.yyyy-mm.naming-authority:unique` para el nombre, donde:

- *yyyy-mm* es el año y el mes en que se estableció la autoridad de asignación de nombres.
- *naming-authority* es la sintaxis inversa del nombre de dominio de Internet de la autoridad de asignación de nombres. Por ejemplo, la autoridad de asignación de

nombres de `iscsi.vmware.com` puede tener el formato de nombre calificado de iSCSI de `iqn.1998-01.com.vmware.iscsi`. El nombre indica que se ha registrado el nombre de dominio `vmware.com` en enero de 1998 e `iscsi` es un subdominio, mantenido por `vmware.com`.

- *unique name* es cualquier nombre que desee usar; por ejemplo, el nombre del host. La autoridad de asignación de nombres debe asegurarse de que todos los nombres asignados después de los dos puntos sean únicos, por ejemplo:
  - `iqn.1998-01.com.vmware.iscsi:name1`
  - `iqn.1998-01.com.vmware.iscsi:name2`
  - `iqn.1998-01.com.vmware.iscsi:name999`

Formato identificador único empresarial

El formato identificador único empresarial (EUI) adopta la forma `eui.16_hex_digits`.

Por ejemplo, `eui.0123456789ABCDEF`.

Los dígitos de 16 hexadecimales son representaciones en texto de números de 64 bits en formato IEEE EUI (identificador único extendido). Los 24 bits superiores son un identificador de empresa que IEEE registra con una empresa determinada. La entidad titular de ese identificador de empresa asigna los 40 bits restantes, que deben ser únicos.

Iniciadores iSCSI

Para acceder a destinos iSCSI, el host ESXi utiliza iniciadores iSCSI.

El iniciador es un software o hardware que se instaló en el host ESXi. El iniciador iSCSI origina la comunicación entre el host y un sistema de almacenamiento iSCSI externo, y envía datos al sistema de almacenamiento.

En el entorno de ESXi, los adaptadores de iSCSI configurados en el host cumplen la función de iniciadores. ESXi es compatible con varios tipos de adaptadores de iSCSI.

Para obtener información sobre cómo configurar y utilizar adaptadores de iSCSI, consulte Capítulo 11 Configurar adaptadores y almacenamiento de iSCSI e iSER.

Adaptador de iSCSI de software

Un adaptador de iSCSI de software es un código de VMware integrado en el VMkernel. Con este adaptador, el host se puede conectar al dispositivo de almacenamiento iSCSI mediante adaptadores de red estándar. El adaptador de iSCSI de software controla el procesamiento de iSCSI mientras se comunica con el adaptador de red. Con el adaptador de iSCSI de software, se puede utilizar tecnología iSCSI sin adquirir hardware especializado.

Adaptador de iSCSI de hardware

Un adaptador de iSCSI de hardware es un adaptador de terceros que asigna procesamiento de iSCSI y de red desde el host. Los adaptadores de iSCSI de hardware se dividen en categorías.

Adaptador de iSCSI de hardware dependiente

Depende de las redes de VMware y de las interfaces de configuración y administración de iSCSI proporcionadas por VMware.

Este tipo de adaptador puede ser una tarjeta que presenta un adaptador de red estándar y una funcionalidad de asignación de iSCSI para el mismo puerto. La funcionalidad de asignación de iSCSI depende de la configuración de red del host para obtener la IP, la dirección MAC y otros parámetros utilizados para sesiones iSCSI. Un ejemplo de un adaptador dependiente es Broadcom 5709 NIC con licencia iSCSI.

Adaptador de iSCSI de hardware independiente

Implementa su propia configuración de redes y de iSCSI, además de sus propias interfaces de administración.

Por lo general, un adaptador de iSCSI de hardware independiente es una tarjeta que presenta solo funcionalidad de asignación de iSCSI o funcionalidad de asignación de iSCSI y funcionalidad de NIC estándar. La funcionalidad de asignación de iSCSI posee una administración de configuración independiente que asigna la IP, la dirección MAC y otros parámetros utilizados para las sesiones iSCSI. Un ejemplo de un adaptador independiente es QLogic QLA4052.

Es posible que deba obtenerse una licencia para los adaptadores de iSCSI de hardware. En caso contrario, podrían no aparecer en la CLI del cliente o de vSphere. Para obtener información sobre licencias, póngase en contacto con el proveedor.

Usar el protocolo iSER con ESXi

Además del iSCSI tradicional, ESXi es compatible con las extensiones de iSCSI para el protocolo RDMA (iSER). Cuando se habilita el protocolo iSER, el marco de iSCSI en el host ESXi puede usar el transporte de acceso de memoria directo remoto (Remote Direct Memory Access, RDMA) en lugar de TCP/IP.

El protocolo iSCSI tradicional transporta comandos SCSI a través de una red TCP/IP entre un iniciador iSCSI en un host y un destino iSCSI en un dispositivo de almacenamiento. El protocolo iSCSI encapsula los comandos y ensambla esos datos en paquetes para la capa de TCP/IP. Al recibir los datos, el protocolo iSCSI desensambla los paquetes de TCP/IP, de modo que sea posible diferenciar los comandos SCSI y entregarlos al dispositivo de almacenamiento.

iSER es diferente del protocolo iSCSI tradicional, ya que sustituye el modelo de transferencia de datos de TCP/IP por el transporte de RDMA. Mediante la tecnología de colocación de datos directa de RDMA, el protocolo iSER puede transferir datos directamente entre los búferes de memoria del host ESXi y los dispositivos de almacenamiento. Este método elimina el procesamiento de TCP/IP innecesario y el copiado de datos, y también puede reducir la latencia y la carga de CPU en el dispositivo de almacenamiento.

En el entorno de iSER, iSCSI funciona exactamente igual que antes, pero usa una interfaz de tejido subyacente de RDMA en lugar de la interfaz basada en TCP/IP.

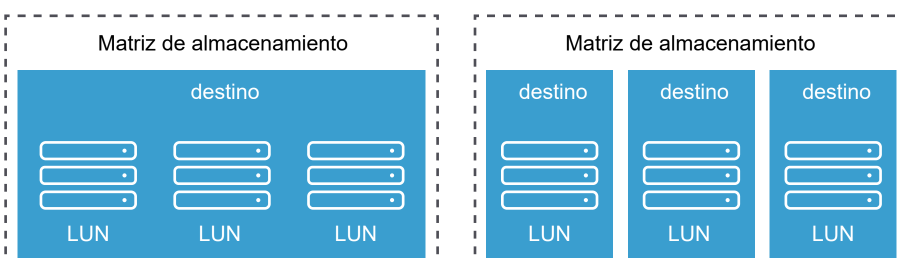
Debido a que el protocolo iSER preserva la compatibilidad con la infraestructura de iSCSI, el proceso de habilitación de iSER en el host ESXi es similar al proceso de iSCSI. Consulte Configurar iSER con ESXi.

Establecer conexiones iSCSI

En el contexto de ESXi, el término destino identifica a una sola unidad de almacenamiento a la que puede acceder el host. Los términos dispositivo de almacenamiento y LUN describen un volumen lógico que representa espacio de almacenamiento en un destino. Por lo general, los términos dispositivo y LUN, en el contexto de ESXi, significan un volumen SCSI presentado al host desde un destino de almacenamiento y disponible para dar formato.

Los distintos proveedores de almacenamiento iSCSI presentan el almacenamiento a los hosts de distintas formas. Algunos proveedores presentan varios LUN en un solo destino, mientras que otros presentan varios destinos con un LUN en cada uno.

Figura 10-1. Destino en comparación con representaciones de LUN



En estos ejemplos, hay tres LUN disponibles en cada una de estas configuraciones. En el primer caso, el host detecta un destino, pero ese destino tiene tres LUN que se pueden utilizar. Cada uno de los LUN representa un volumen de almacenamiento individual. En el segundo caso, el host detecta tres destinos diferentes, cada uno con un LUN.

Los iniciadores iSCSI basados en host establecen conexiones a cada destino. Los sistemas de almacenamiento con un solo destino con varios LUN tienen tráfico a todos los LUN en una sola conexión. Con un sistema que tiene tres destinos con un LUN en cada uno, el host utiliza conexiones distintas a los tres LUN.

Esta información es útil cuando se intenta agregar tráfico de almacenamiento en varias conexiones desde el host con varios adaptadores de iSCSI. Puede establecer el tráfico de un destino en un adaptador concreto y utilizar otro adaptador para el tráfico en otra instancia de destino.

Tipos de sistema de almacenamiento iSCSI

ESXi admite distintas matrices y sistemas de almacenamiento.

Entre los tipos de almacenamiento que admite un host se encuentran activo-activo, activo-pasivo y compatible con ALUA.

Sistema de almacenamiento activo-activo

Permite acceder simultáneamente a los LUN en todos los puertos de almacenamiento que están disponibles sin una degradación significativa del rendimiento. Todas las rutas de acceso siempre están activas, a menos que se produzca un error en alguna.

Sistema de almacenamiento activo-pasivo

Un sistema en el cual un procesador de almacenamiento proporciona acceso de forma activa a un LUN determinado. Los otros procesadores actúan como copia de seguridad del LUN y pueden proporcionar acceso activamente a otras operaciones de E/S del LUN. Las operaciones de E/S pueden enviarse correctamente solo a un puerto activo de un LUN determinado. Si el acceso a través del puerto de almacenamiento activo genera errores, uno de los procesadores de almacenamiento pasivos puede activarse mediante los servidores que acceden a él.

Sistema de almacenamiento asimétrico

Admite acceso asimétrico a unidades lógicas (ALUA). Los sistemas de almacenamiento compatibles con ALUA ofrecen diferentes niveles de acceso por puerto. Con ALUA, los hosts pueden determinar los estados de los puertos de destino y priorizar las rutas de acceso. El host utiliza algunas de las rutas de acceso activas como principales y otras como secundarias.

Sistema de almacenamiento de puerto virtual

Admite el acceso a todos los LUN disponibles a través de un solo puerto virtual. Los sistemas de almacenamiento virtual son dispositivos de almacenamiento activo-activo, pero ocultan sus distintas conexiones a través de un solo puerto. La habilitación de múltiples rutas de ESXi no crea varias conexiones a partir de un puerto específico al almacenamiento de forma predeterminada. Algunos proveedores de almacenamiento suministran administradores de sesión para establecer y administrar varias conexiones al almacenamiento. Estos sistemas de almacenamiento controlan la conmutación por error de puertos y el equilibrio de la conexión de forma transparente. Esta capacidad se denomina a menudo conmutación por error transparente.

Detectar, autenticar y controlar el acceso

Se pueden utilizar distintos mecanismos para detectar el almacenamiento y limitar el acceso a él.

El host y el sistema de almacenamiento iSCSI se deben configurar para que admitan la directiva de control de acceso al almacenamiento del usuario.

Detección

Una sesión de detección es parte del protocolo iSCSI y devuelve el conjunto de destinos al que se puede acceder en un sistema de almacenamiento iSCSI. Los dos tipos de detección disponibles en ESXi son dinámica y estática. La detección dinámica obtiene una lista de destinos accesibles del sistema de almacenamiento de iSCSI. La detección estática solo puede acceder a un destino concreto mediante el nombre y la dirección del destino.

Para obtener más información, consulte Configurar la detección dinámica o estática para iSCSI e iSER en un host ESXi.

Autenticación

Los sistemas de almacenamiento iSCSI autentican un iniciador mediante un par de nombre y clave. ESXi es compatible con el protocolo de autenticación de CHAP. Para utilizar la autenticación de CHAP, el host ESXi y el sistema de almacenamiento iSCSI deben tener CHAP habilitado y disponer de credenciales comunes.

Para obtener información sobre cómo habilitar CHAP, consulte Configurar los parámetros de CHAP para los adaptadores de almacenamiento de iSCSI o iSER.

Control de acceso

Control de acceso es una directiva configurada en el sistema de almacenamiento iSCSI. La mayoría de las implementaciones admiten uno o más de tres tipos de control de acceso:

- Por nombre de iniciador
- Por dirección IP
- Por el protocolo CHAP

Solo los iniciadores que cumplen con todas las reglas pueden acceder al volumen iSCSI.

Utilizar solo CHAP para el control de acceso puede desacelerar el proceso de volver a examinar debido a que el host ESXi puede detectar todos los destinos, pero en el paso de autenticación. El proceso de volver a examinar de iSCSI funciona más rápido si el host detecta solo los destinos que puede autenticar.

Cómo acceden las máquinas virtuales a los datos en una SAN iSCSI

ESXi almacena los archivos del disco de una máquina virtual en un almacén de datos de VMFS que reside en un dispositivo de almacenamiento SAN. Cuando los sistemas operativos invitados de la máquina virtual emiten comandos SCSI a sus discos virtuales, la capa de virtualización SCSI traduce esos comandos a operaciones de archivos VMFS.

Cuando una máquina virtual interactúa con su disco virtual almacenado en una SAN, se llevan a cabo los siguientes procesos:

1 Cuando el sistema operativo invitado de una máquina virtual lee o escribe en el disco SCSI, emite comandos SCSI al disco virtual.
2 Los controladores de dispositivos en el sistema operativo de la máquina virtual se comunican con las controladoras SCSI virtuales.
3 La controladora SCSI virtual reenvía los comandos al VMkernel.
4 El VMkernel realiza las siguientes tareas.
   a Busca un archivo de disco virtual apropiado en el volumen VMFS.
   b Asigna las solicitudes de los bloques en el disco virtual en bloques del dispositivo físico apropiado.
   c Envía la solicitud de E/S modificada desde el controlador del dispositivo en el VMkernel hacia el iniciador iSCSI (hardware o software).
5 Si el iniciador iSCSI es un adaptador de iSCSI de hardware, sea independiente o dependiente, el adaptador realiza las siguientes tareas.
   a Encapsula las solicitudes de E/S en unidades de datos de protocolo (PDU) de iSCSI.
   b Encapsula PDU de iSCSI en paquetes TCP/IP.
   c Envía paquetes IP por Ethernet al sistema de almacenamiento iSCSI.
6 Si el iniciador iSCSI es un adaptador de iSCSI del software, ocurre lo siguiente.
   a El iniciador iSCSI encapsula las solicitudes de E/S en PDU de iSCSI.
   b El iniciador envía PDU de iSCSI a través de conexiones TCP/IP.
   c La pila de TCP/IP del VMkernel retransmite los paquetes TCP/IP a la NIC física.
   d La NIC física envía paquetes IP por Ethernet al sistema de almacenamiento iSCSI.
7 Los enrutadores y los conmutadores Ethernet de la red transmiten la solicitud al dispositivo de almacenamiento adecuado.

Corregir errores

Para proteger la integridad de los datos y encabezados iSCSI, el protocolo iSCSI define los métodos de corrección de errores conocidos como resúmenes de encabezados y resúmenes de datos.

Ambos parámetros están deshabilitados de forma predeterminada, pero es posible habilitarlos. Estos resúmenes pertenecen, respectivamente, al encabezado y a los datos de SCSI que se transfieren entre los iniciadores iSCSI y los destinos, en ambas direcciones.

Los resúmenes de encabezado y datos comprueban la integridad de los datos no criptográficos, más allá de las comprobaciones de integridad que proporcionan otras capas de redes, como TCP y Ethernet. Los resúmenes comprueban la ruta de acceso de comunicación completa, incluidos todos los elementos que pueden cambiar el tráfico en el nivel de la red, como los enrutadores, los conmutadores y los proxy.

La existencia y el tipo de los resúmenes se negocian cuando se establece una conexión iSCSI. Cuando el iniciador y el destino acuerdan una configuración de resumen, este resumen debe utilizarse para todo el tráfico entre ellos.

Habilitar los resúmenes de encabezado y datos requiere un procesamiento adicional tanto para el iniciador como para el destino, y puede afectar la capacidad de proceso y el rendimiento de la CPU.

Nota Los sistemas que utilizan procesadores Intel Nehalem descargan los cálculos del resumen de iSCSI, lo que reduce el impacto sobre el rendimiento.

Para obtener información sobre cómo habilitar los resúmenes de datos y encabezado, consulte Configurar los parámetros avanzados de iSCSI.

Configurar adaptadores y almacenamiento de iSCSI e iSER

11

Antes de que ESXi pueda trabajar con una SAN de iSCSI, se debe configurar un entorno iSCSI.

El proceso de preparación del entorno iSCSI incluye los siguientes pasos:

Paso	Detalles
Configurar el almacenamiento iSCSI	Para obtener más información, consulte la documentación del proveedor de almacenamiento. Además, siga estas recomendaciones: ■ Restricciones y recomendaciones de SAN de iSCSI para ESXi ■ Capítulo 13 Prácticas recomendadas de almacenamiento iSCSI
Configurar adaptadores de iSCSI/ iSER	Utilice el flujo de trabajo correspondiente para configurar el adaptador: ■ Configurar adaptadores de iSCSI de hardware independientes ■ Configurar los adaptadores de iSCSI de hardware dependiente ■ Configurar adaptador de iSCSI de software ■ Configurar iSER con ESXi
Crear un almacén de datos en el almacenamiento iSCSI	Crear almacenes de datos

Este capítulo incluye los siguientes temas:

- Restricciones y recomendaciones de SAN de iSCSI para ESXi
- Configurar los parámetros de iSCSI para adaptadores
- Configurar adaptadores de iSCSI de hardware independientes
- Configurar los adaptadores de iSCSI de hardware dependiente
- Configurar adaptador de iSCSI de software
- Configurar iSER con ESXi
- Modificar propiedades generales de los adaptadores de iSCSI o iSER
- Configurar la seguridad de red para iSCSI e iSER
- Usar tramas gigantes con iSCSI y con iSER
- Configurar la detección dinámica o estática para iSCSI e iSER en un host ESXi
- Quitar destinos iSCSI dinámicos o estáticos
- Configurar los parámetros de CHAP para los adaptadores de almacenamiento de iSCSI o iSER

- Configurar los parámetros avanzados de iSCSI
- Administrar sesiones de iSCSI

Restricciones y recomendaciones de SAN de iSCSI para ESXi

Para que funcione correctamente con una SAN de iSCSI, el entorno de ESXi debe seguir recomendaciones específicas. Además, existen varias restricciones cuando se utiliza ESXi con SAN de iSCSI.

Recomendaciones para almacenamiento iSCSI

- Compruebe que el host ESXi sea compatible con el firmware y el hardware de almacenamiento SAN de iSCSI. Para acceder a una lista actualizada, consulte la *Guía de compatibilidad de VMware*.
- Para asegurarse de que el host reconozca los LUN durante el inicio, configure todos los destinos de almacenamiento iSCSI de forma tal que el host pueda acceder a ellos y usarlos. Configure el host de forma tal que pueda detectar todos los destinos iSCSI disponibles.
- A menos que utilice servidores sin disco, configure una partición de diagnóstico en un almacenamiento local. Si tiene servidores sin disco que arrancan desde una SAN iSCSI, consulte Recomendaciones generales para el arranque desde SAN iSCSI para obtener información sobre las particiones de diagnóstico con iSCSI.
- Establezca el controlador de la controladora SCSI en el sistema operativo invitado con una cola lo suficientemente grande.
- En máquinas virtuales que ejecutan Microsoft Windows, aumente el valor del parámetro de SCSI `TimeoutValue`. Cuando se configura este parámetro, las máquinas virtuales de Windows pueden tolerar mejor los retrasos en E/S que se generan como resultado de una conmutación por error de la ruta de acceso. Para obtener información, consulte Establecer el tiempo de espera en un sistema operativo invitado Windows.
- Configure el entorno para que tenga un solo almacén de datos de VMFS por cada LUN.

Restricciones de almacenamiento iSCSI

- ESXi no es compatible con dispositivos de cinta conectados a iSCSI.
- No se puede usar un software de múltiples rutas de máquina virtual para realizar el equilibrio de carga de E/S de un único LUN físico.
- ESXi no admite múltiples rutas cuando se combinan adaptadores de hardware independiente con adaptadores de hardware dependiente o de software.

Configurar los parámetros de iSCSI para adaptadores

Para que el host ESXi pueda detectar el almacenamiento de iSCSI, se deben configurar los adaptadores de iSCSI. Al configurar los adaptadores, se establecen varios parámetros de iSCSI.

redes iSCSI

Para ciertos tipos de adaptadores de iSCSI, debe configurar redes de VMkernel.

Puede comprobar la configuración de red con la utilidad `vmkping`.

El adaptador de iSCSI de hardware independiente no requiere redes de VMkernel. Puede configurar los parámetros de red, como una dirección IP, una máscara de subred y una puerta de enlace predeterminada en el adaptador de iSCSI de hardware independiente.

Todos los tipos de adaptadores de iSCSI admiten protocolos IPv4 e IPv6.

Adaptador de iSCSI (vmhba)	Descripción	Redes VMkernel	Configuración de red del adaptador
Adaptador de iSCSI de hardware independiente	Adaptador de terceros que descarga la administración y el procesamiento de red e iSCSI del host.	No son obligatorias.	Para obtener información, consulte Editar la configuración de red para iSCSI de hardware.
Adaptador de iSCSI de software	Utiliza NIC estándar para conectar el host a un destino iSCSI remoto en la red IP.	Requerido. Para obtener información, consulte Configurar la seguridad de red para iSCSI e iSER.	N/C
Adaptador de iSCSI de hardware dependiente	Adaptador de terceros que depende de las interfaces de administración y configuración de iSCSI y de las redes de VMware.	Obligatorio Para obtener información, consulte Configurar la seguridad de red para iSCSI e iSER.	N/C
Adaptador de iSER de VMware	Utiliza un adaptador de red compatible con RDMA para conectar el host a un destino iSCSI remoto.	Obligatorio Para obtener información, consulte Configurar la seguridad de red para iSCSI e iSER.	N/C

Métodos de detección

Para todos los tipos de adaptadores de iSCSI, se debe establecer la dirección de detección dinámica o detección estática. Además, debe proporcionar un nombre de destino del sistema de almacenamiento. Para iSCSI de software e iSCSI de hardware dependiente, se puede hacer ping en la dirección con `vmkping`.

Consulte Configurar la detección dinámica o estática para iSCSI e iSER en un host ESXi.

Autenticación de CHAP

Habilite el parámetro CHAP en el iniciador y en el lado del sistema de almacenamiento. Una vez habilitada la autenticación, se aplica a todos los destinos que aún no se detectaron, pero no se aplica a los destinos ya detectados.

Consulte Configurar los parámetros de CHAP para los adaptadores de almacenamiento de iSCSI o iSER.

Configurar adaptadores de iSCSI de hardware independientes

Un adaptador de iSCSI de hardware independiente es un adaptador de terceros especializado capaz de acceder al almacenamiento iSCSI mediante TCP/IP. Este adaptador de iSCSI controla todo el procesamiento y la administración de red e iSCSI para el sistema ESXi.

Requisitos previos

- Compruebe si el adaptador debe tener una licencia.
- Instale el adaptador en el host ESXi.

Para obtener información sobre las licencias, la instalación y las actualizaciones de firmware, consulte la documentación del proveedor.

El proceso de configurar el adaptador de iSCSI de hardware independiente incluye estos pasos.

Paso	Descripción
Ver adaptadores de iSCSI de hardware independientes	Puede ver un adaptador de iSCSI de hardware independiente para comprobar que esté instalado correctamente y listo para ser configurado.
Modificar propiedades generales de los adaptadores de iSCSI o iSER	Si es necesario, cambie el nombre de iSCSI predeterminado y el alias asignado a los adaptadores de iSCSI. En el caso de los adaptadores de iSCSI de hardware independientes, también se puede cambiar la configuración IP predeterminada.
Editar la configuración de red para iSCSI de hardware	Cambie la configuración de red predeterminada de modo que el adaptador quede configurado correctamente para la SAN de iSCSI.
Configurar la detección dinámica o estática para iSCSI e iSER en un host ESXi	Configure la detección dinámica. Con la detección dinámica, cada vez que el iniciador se contacte con el sistema de almacenamiento iSCSI especificado, le enviará una solicitud de SendTargets. El sistema iSCSI le responde al iniciador y le suministra una lista de destinos disponibles. Además del método de detección dinámica, se puede utilizar una detección estática e introducir manualmente la información de los destinos.
Configurar CHAP para un adaptador de almacenamiento de iSCSI o iSER	Si el entorno de iSCSI utiliza el protocolo de autenticación por desafío mutuo (Challenge Handshake Authentication Protocol, CHAP), configúrelo para el adaptador.
Habilitar tramas gigantes para iSCSI de hardware independiente	Si su entorno iSCSI es compatible con tramas gigantes, habilítelas para el adaptador.

Ver adaptadores de iSCSI de hardware independientes

En el host ESXi, puede ver un adaptador de iSCSI de hardware independiente para comprobar que esté instalado correctamente y listo para ser configurado.

Después de instalar un adaptador de iSCSI de hardware independiente en el host, aparecerá en la lista de adaptadores de almacenamiento disponibles para su configuración. Es posible ver sus propiedades.

Requisitos previos

Privilegio necesario: **Host.Configuración.Configuración de partición de almacenamiento**

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento**.

   Si está instalado, el adaptador de iSCSI de hardware aparecerá en la lista de adaptadores de almacenamiento.

4 Seleccione el adaptador que desea ver.

   Aparecen los detalles predeterminados del adaptador.

Información del adaptador	Descripción
Modelo	Modelo del adaptador.
Nombre iSCSI	Nombre único formado según los estándares de iSCSI que identifica al adaptador de iSCSI. Puede editar el nombre iSCSI.
Alias iSCSI	Nombre alternativo que se utiliza en lugar del nombre iSCSI. Puede editar el alias iSCSI.
Dirección IP	Dirección asignada al HBA de iSCSI.
Destinos	Cantidad de destinos a los que se accede a través del adaptador.
Dispositivos	Todos los dispositivos de almacenamiento o LUN a los que puede acceder el adaptador.
Rutas de acceso	Todas las rutas de acceso que utiliza el adaptador para acceder a dispositivos de almacenamiento.

Editar la configuración de red para iSCSI de hardware

Después de instalar un adaptador de iSCSI de hardware independiente en un host ESXi, es posible que deba cambiar la configuración de red predeterminada para configurarlo correctamente para la SAN iSCSI.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione el adaptador (vmhba#) que desea configurar.

4 Haga clic en la pestaña **Configuración de red** y luego en **Editar**.

5 En la sección de configuración de IPv4, deshabilite IPv6 o seleccione el método para obtener las direcciones IP.

Nota Las opciones de DHCP automático y estático son mutuamente exclusivas.

Opción	Descripción
Sin configuración de IPv4	Deshabilite IPv4.
Obtener configuración de IPv4 automáticamente	Use DHCP para obtener la configuración de IP.
Usar configuración de IPv4 estática	Escriba la dirección IP, la máscara de subred y la puerta de enlace predeterminada IPv4 para el adaptador de iSCSI.

6 En la sección de configuración de IPv6, deshabilite IPv6 o seleccione una opción adecuada para obtener las direcciones IPv6.

Nota Las opciones automática y estática son mutuamente exclusivas.

Opción	Descripción
Sin configuración IPv6	Deshabilite IPv6.
Habilitar IPv6	Seleccione una opción para obtener las direcciones IPv6.
Obtener las direcciones IPv6 automáticamente por medio de DHCP	Use DHCP para obtener las direcciones IPv6.
Obtener las direcciones IPv6 automáticamente por medio del anuncio de enrutador	Use el anuncio de enrutador para obtener las direcciones IPv6.
Anular dirección local de vínculo para IPv6	Anule la dirección IP local de vínculo con la configuración de una dirección IP estática.
Direcciones IPv6 estáticas	a Haga clic en **Agregar** para agregar una nueva dirección IPv6. b Introduzca la dirección IPv6 y la longitud del prefijo de subred, y haga clic en **Aceptar**.

7 En la sección de configuración de DNS, proporcione las direcciones IP de un servidor DNS preferido y un servidor DNS alternativo.

Debe proporcionar ambos valores.

Configurar los adaptadores de iSCSI de hardware dependiente

Un adaptador de iSCSI de hardware dependiente es un adaptador de terceros que depende de las redes de VMware, así como de las interfaces de administración y configuración de iSCSI que proporciona VMware.

Un ejemplo de adaptador de iSCSI dependiente es una NIC Broadcom 5709. Cuando está instalado en un host, presenta sus dos componentes, un adaptador de red estándar y un motor iSCSI, en el mismo puerto. El motor iSCSI aparece en la lista de adaptadores de almacenamiento como un adaptador de iSCSI (vmhba).

El adaptador de iSCSI está habilitado de forma predeterminada. Para que funcione, debe conectarlo mediante un adaptador de VMkernel (vmk) virtual a un adaptador de red física (vmnic) que esté asociado con él. A continuación, puede configurar el adaptador de iSCSI.

Tras configurar el adaptador de iSCSI de hardware dependiente, los datos de detección y autenticación pasan a través de la conexión de red. El tráfico iSCSI pasa por el motor iSCSI, sin pasar por la red.

El proceso completo de instalación y configuración de los adaptadores de iSCSI de hardware dependiente involucran varios pasos.

Paso	Descripción
Ver adaptadores de iSCSI de hardware dependiente	Se puede ver un adaptador de iSCSI de hardware dependiente para comprobar que esté correctamente cargado.
Modificar propiedades generales de los adaptadores de iSCSI o iSER	Si es necesario, cambie el nombre iSCSI predeterminado y el alias asignado al adaptador.
Determinar la asociación entre iSCSI y los adaptadores de red	Puede crear conexiones de red para vincular adaptadores de iSCSI dependientes y adaptadores de red física. Para crear las conexiones correctamente, determine el nombre de la NIC física con la que está asociado el adaptador de iSCSI de hardware dependiente.
Configurar el enlace de puertos de iSCSI o iSER	Configure conexiones para el tráfico entre el componente iSCSI y los adaptadores de red física. El proceso de configuración de estas conexiones se denomina enlace de puerto.
Configurar la detección dinámica o estática para iSCSI e iSER en un host ESXi	Configure la detección dinámica. Con la detección dinámica, cada vez que el iniciador se contacte con el sistema de almacenamiento iSCSI especificado, le enviará una solicitud de SendTargets. El sistema iSCSI le responde al iniciador y le suministra una lista de destinos disponibles. Además del método de detección dinámica, se puede utilizar una detección estática e introducir manualmente la información de los destinos.
Configurar CHAP para un adaptador de almacenamiento de iSCSI o iSER	Si el entorno de iSCSI utiliza el protocolo de autenticación por desafío mutuo (Challenge Handshake Authentication Protocol, CHAP), configúrelo para el adaptador.
Configurar CHAP para un destino	También puede configurar diferentes credenciales CHAP para cada dirección de detección o destino estático.
Habilitar tramas gigantes para redes	Si su entorno iSCSI es compatible con tramas gigantes, habilítelas para el adaptador.

Consideraciones sobre iSCSI de hardware dependiente

Cuando se utilizan adaptadores de iSCSI de hardware dependiente con ESXi, aplican ciertas consideraciones.

- Cuando se utiliza cualquier adaptador de iSCSI de hardware dependiente, los informes de rendimiento de una NIC asociada con el adaptador pueden mostrar poca o ninguna actividad, incluso cuando hay demasiado tráfico iSCSI. Este comportamiento ocurre porque el tráfico iSCSI omite la pila de redes normal.
- Si utiliza un conmutador virtual de terceros, por ejemplo, Cisco Nexus 1000V DVS, deshabilite la fijación automática. En su lugar, utilice la fijación manual, y asegúrese de conectar un adaptador VMkernel (vmk) a una NIC física (vmnic) adecuada. Para obtener información, consulte la documentación del proveedor del conmutador virtual.
- El adaptador Broadcom iSCSI realiza el reensamblaje de datos en el hardware, el cual tiene espacio de búfer limitado. Cuando utilice el adaptador Broadcom iSCSI en una red congestionada o con una carga pesada, habilite el control de flujo para evitar la degradación del rendimiento.

  El control de flujo administra la tasa de transmisión de datos entre dos nodos para evitar que un remitente rápido sature a un receptor lento. Para obtener los mejores resultados, habilite el control de flujo en los extremos de la ruta de acceso de E/S, en los hosts y en los sistemas de almacenamiento iSCSI.

  Para habilitar el control de flujo para el host, utilice el comando `esxcli system module parameters`. Para obtener detalles, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/1013413
- Los adaptadores de hardware dependiente son compatibles con IPv4 e IPv6.

Ver adaptadores de iSCSI de hardware dependiente

En un host ESXi, puede ver un adaptador de iSCSI de hardware dependiente para comprobar que esté correctamente cargado.

Si hay un adaptador de iSCSI de hardware dependiente (vmhba#) instalado, aparece en la lista de adaptadores de almacenamiento en una categoría, por ejemplo, Adaptador de iSCSI Broadcom. Si el adaptador de hardware dependiente no aparece en la lista de adaptadores de almacenamiento, compruebe si necesita una licencia. Consulte la documentación del proveedor.

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento**.

4 Seleccione el adaptador (vmhba#) para verlo.

Aparecen los detalles predeterminados del adaptador, incluidos el nombre iSCSI, alias iSCSI y el estado.

Pasos siguientes

Aunque el adaptador de iSCSI dependiente esté habilitado de forma predeterminada, para que funcione, se debe configurar la red para el tráfico iSCSI y enlazar el adaptador al puerto VMkernel de iSCSI correspondiente. A continuación, se configuran las direcciones de detección y los parámetros CHAP.

Determinar la asociación entre iSCSI y los adaptadores de red

En un host ESXi, las conexiones de red enlazan los adaptadores de red físicos y de iSCSI dependientes. Para crear las conexiones correctamente, se debe determinar el nombre de la NIC física con la que está asociado el adaptador de iSCSI de hardware dependiente.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento**.

4 Seleccione el adaptador de iSCSI y haga clic en la pestaña **Enlace de puertos de red** en Detalles del adaptador.

5 Haga clic en **Agregar**.

El adaptador de red (vmnic#) que corresponde al adaptador de iSCSI dependiente aparece en la columna Adaptador de red físico.

Pasos siguientes

Si la columna Adaptador VMkernel está vacía, cree un adaptador vmk# para el adaptador de red físico (vmnic#) y vincúlelo con el iSCSI de hardware dependiente asociado. Consulte Configurar la seguridad de red para iSCSI e iSER.

Configurar adaptador de iSCSI de software

La implementación de iSCSI basado en software permite utilizar NIC estándar para conectar el host a un destino iSCSI remoto en la red IP. El adaptador de iSCSI de software incorporado en ESXi facilita esta conexión gracias a la comunicación con la NIC física a través de la pila de red.

Al utilizar adaptadores de iSCSI de software, tenga en cuenta lo siguiente:

- Designe un adaptador de red independiente para iSCSI. No utilice iSCSI para adaptadores de 100 Mbps o más lentos.

- Evite codificar de forma rígida el nombre del adaptador de software, vmhbaXX, en los scripts. Es posible que el nombre cambie de una versión de ESXi a otra. El cambio podría causar errores en sus scripts existentes si usan el nombre antiguo codificado de forma rígida. El cambio de nombre no afecta el comportamiento del adaptador de software de iSCSI.

El proceso de configuración de un adaptador de iSCSI de software involucra varios pasos.

Paso	Descripción
Activar o deshabilitar el adaptador de iSCSI de software	Active el adaptador de iSCSI de software de modo que el host pueda utilizarlo para acceder al almacenamiento iSCSI.
Modificar propiedades generales de los adaptadores de iSCSI o iSER	Si es necesario, cambie el nombre iSCSI predeterminado y el alias asignado al adaptador.
Configurar el enlace de puertos de iSCSI o iSER	Configure conexiones para el tráfico entre el componente iSCSI y los adaptadores de red física. El proceso de configuración de estas conexiones se denomina enlace de puerto.
Configurar la detección dinámica o estática para iSCSI e iSER en un host ESXi	Configure la detección dinámica. Con la detección dinámica, cada vez que el iniciador se contacte con el sistema de almacenamiento iSCSI especificado, le enviará una solicitud de SendTargets. El sistema iSCSI le responde al iniciador y le suministra una lista de destinos disponibles. Además del método de detección dinámica, se puede utilizar una detección estática e introducir manualmente la información de los destinos.
Configurar CHAP para un adaptador de almacenamiento de iSCSI o iSER	Si el entorno de iSCSI utiliza el protocolo de autenticación por desafío mutuo (Challenge Handshake Authentication Protocol, CHAP), configúrelo para el adaptador.
Configurar CHAP para un destino	También puede configurar diferentes credenciales CHAP para cada dirección de detección o destino estático.
Habilitar tramas gigantes para redes	Si su entorno iSCSI es compatible con tramas gigantes, habilítelas para el adaptador.

Activar o deshabilitar el adaptador de iSCSI de software

Se debe activar el adaptador de iSCSI de software para que el host ESXi pueda utilizarlo para acceder al almacenamiento iSCSI. Si no necesita el adaptador de iSCSI de software después de la activación, puede deshabilitarlo.

Se puede activar un solo adaptador de iSCSI de software únicamente.

Requisitos previos

Privilegio necesario: **Host.Configuración.Configuración de partición de almacenamiento**

Nota Si se arranca desde iSCSI utilizando el adaptador de iSCSI de software, el adaptador queda habilitado y la configuración de red se crea en el primer arranque. Si se deshabilita el adaptador, se volverá a habilitar cada vez que se arranque el host.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 Habilite o deshabilite el adaptador.

Opción	Descripción
Habilitar el adaptador de iSCSI de software	a En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y, a continuación, en el icono **Agregar**. b Seleccione **Adaptador de iSCSI de software** y confirme que desea agregar el adaptador. El adaptador de iSCSI de software (vmhba#) está habilitado y aparece en la lista de adaptadores de almacenamiento. Después de habilitar el adaptador, el host le asigna el nombre iSCSI predeterminado. Ahora puede completar la configuración del adaptador.
Deshabilitar el adaptador de iSCSI de software	a En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione el adaptador (vmhba#) que desea deshabilitar. b Haga clic en la pestaña **Propiedades**. c Haga clic en **Deshabilitar** y confirme que desea deshabilitar el adaptador. El estado indica que el adaptador está deshabilitado. d Reinicie el host. Después del reinicio, el adaptador ya no aparece en la lista de adaptadores de almacenamiento. Los dispositivos de almacenamiento asociados con el adaptador se vuelven inaccesibles. Puede activar el adaptador más adelante.

Configurar iSER con ESXi

Además del iSCSI tradicional, ESXi es compatible con las extensiones de iSCSI para el protocolo RDMA (iSER). Cuando se habilita el protocolo iSER, el marco de iSCSI en el host ESXi puede usar el transporte de acceso de memoria directo remoto (Remote Direct Memory Access, RDMA) en lugar de TCP/IP. Puede configurar iSER en el host ESXi.

Para obtener más información sobre el protocolo iSER, consulte Usar el protocolo iSER con ESXi.

El proceso completo de instalación y configuración de iSER de VMware involucra varios pasos.

Paso	Descripción
Instalar y ver un adaptador de red compatible con RDMA	Para configurar iSER con ESXi, primero debe instalar un adaptador de red compatible con RDMA, por ejemplo, Mellanox Technologies MT27700 Family ConnectX-4. Después de instalar este tipo de adaptador, vSphere Client muestra sus dos componentes, un adaptador RDMA y un adaptador de red físico `vmnic#`.
Habilitar el adaptador de iSER de VMware	Para poder utilizar el adaptador compatible con RDMA para iSCSI, utilice `esxcli` para habilitar el componente de almacenamiento iSER de VMware. El componente aparece en vSphere Client como un adaptador de almacenamiento `vmhba#` en la categoría Adaptador de iSCSI de VMware a través de RDMA (iSER).
Modificar propiedades generales de los adaptadores de iSCSI o iSER	Si es necesario, cambie el nombre y el alias predeterminados que se asignaron al adaptador de almacenamiento de iSER `vmhba#`.

Paso	Descripción
Configurar el enlace de puertos de iSCSI o iSER	Debe crear conexiones de red para vincular el adaptador de almacenamiento de iSER `vmhba#` y el adaptador de red compatible con RDMA `vmnic#`. El proceso de configuración de estas conexiones se denomina enlace de puerto. **Nota** iSER no es compatible con la agrupación de NIC. Al configurar el enlace de puertos, utilice un solo adaptador de RDMA por vSwitch.
Configurar la detección dinámica o estática para iSCSI e iSER en un host ESXi	Configure la detección dinámica o estática para el adaptador de almacenamiento de iSER `vmhba#`. Con la detección dinámica, cada vez que el iniciador se contacte con el sistema de almacenamiento iSER especificado, le enviará una solicitud de SendTargets. El sistema iSER le responderá al iniciador y le suministrará una lista de destinos disponibles. Con la detección estática, debe introducir manualmente la información de los destinos.
Configurar CHAP para un adaptador de almacenamiento de iSCSI o iSER	Si el entorno utiliza el protocolo de autenticación por desafío mutuo (Challenge Handshake Authentication Protocol, CHAP), configúrelo para el adaptador de almacenamiento de iSER `vmhba#`.
Configurar CHAP para un destino	También puede configurar diferentes credenciales CHAP para cada dirección de detección o destino estático.
Habilitar tramas gigantes para redes	Si el entorno admite tramas gigantes, habilite esas tramas para el adaptador de almacenamiento de iSER `vmhba#`.

Instalar y ver un adaptador de red compatible con RDMA

ESXi es compatible con adaptadores de red compatibles con RDMA, por ejemplo, la familia MT27700 de Mellanox Technologies ConnectX-4. Después de instalar este adaptador en el host, vSphere Client muestra sus dos componentes, un adaptador RDMA y un adaptador de red físico.

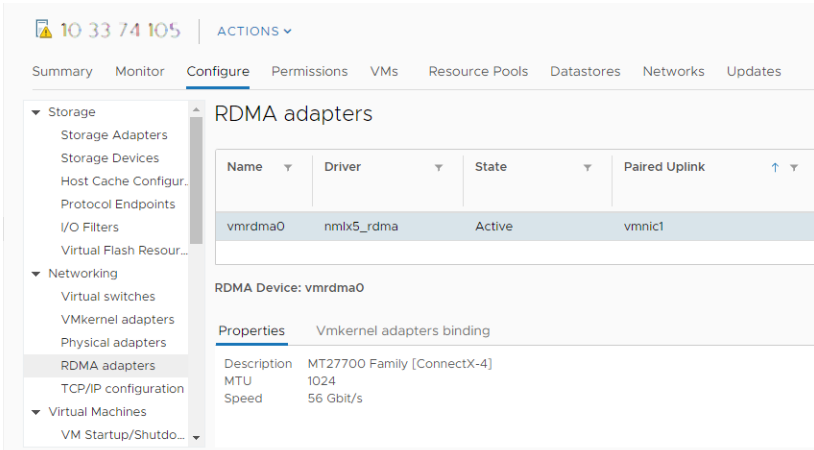
Puede utilizar vSphere Client para ver el adaptador RDMA y su adaptador de red correspondiente.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 En **Redes**, haga clic en **Adaptadores RDMA**.

   En este ejemplo, el adaptador RDMA aparece en la lista como `vmrdma0`. La columna **Vínculo superior emparejado** muestra el componente de red como el adaptador de red físico `vmnic1`.



3 Para comprobar la descripción del adaptador, seleccione el adaptador RDMA de la lista y haga clic en la pestaña **Propiedades**.

Resultados

Puede utilizar el componente de red `vmnic#` del adaptador para configuraciones de almacenamiento como iSER o NVMe over RDMA. Para ver los pasos de configuración de iSER, consulte Configurar iSER con ESXi. Para obtener información sobre NVMe over RDMA, consulte Configurar adaptadores para el almacenamiento de NVMe over RDMA (RoCE V2).

Habilitar el adaptador de iSER de VMware

Para poder utilizar el adaptador compatible con RDMA para iSCSI, utilice `esxcli` para habilitar el componente de almacenamiento iSER de VMware. Después de habilitar el componente, aparece en vSphere Client como un adaptador de almacenamiento de `vmhba#` en la categoría Adaptador VMware iSCSI a través de RDMA (iSER).

Requisitos previos

- Asegúrese de que el almacenamiento iSCSI sea compatible con el protocolo iSER.
- Instale al adaptador compatible con RDMA en el host ESXi. Para obtener información, consulte Instalar y ver un adaptador de red compatible con RDMA.
- Para los adaptadores compatibles con RDMA que admiten RDMA sobre Ethernet convergente (RoCE), determine la versión de RoCE que utiliza el adaptador.
- Use el conmutador compatible con RDMA.
- Habilite el control de flujo en el host ESXi. Para habilitar el control de flujo para el host, utilice el comando `esxcli system module parameters`. Para obtener información detallada, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/1013413.
- Asegúrese de configurar los puertos de conmutador RDMA para crear conexiones sin pérdida entre el iniciador iSER y el destino.

Procedimiento

1 Use ESXi Shell o vSphere CLI para habilitar el adaptador de almacenamiento de VMware iSER y establecer su versión de RoCE.

   a Habilite el adaptador de almacenamiento de iSER.

      ```
      esxcli rdma iser add
      ```

   b Compruebe que se haya agregado el adaptador de iSER.

      ```
      esxcli iscsi adapter list
      ```

      Los resultados son similares al siguiente.

      ```
      Adapter Driver State UID Description
      ------- ------ ------- ------------- -------------------------------------
      vmhba64 iser unbound iscsi.vmhba64 VMware iSCSI over RDMA (iSER) Adapter
      ```

   c Especifique la versión de RoCE que utiliza iSER para conectarse a la instancia de destino.

      Utilice la versión de RoCE del adaptador compatible con RDMA. El comando que introduzca es similar al siguiente:

      ```
      esxcli rdma iser params set -a vmhba64 -r 1
      ```

      Cuando el comando se completa, aparece un mensaje similar al siguiente en el registro de VMkernel.

      ```
      vmkernel.0:2020-02-18T18:26:15.949Z cpu6:2100717 opID=45abe37e)iser: iser_set_roce:
      Setting roce type: 1 for vmhba: vmhba64
      vmkernel.0:2020-02-18T18:26:15.949Z cpu6:2100717 opID=45abe37e)iser: iser_set_roce:
      Setting rdma port: 3260 for vmhba: vmhba64
      ```

      Si no se especifica la versión de RoCE, el host predeterminado es la versión de RoCE más alta que admite el adaptador compatible con RDMA.

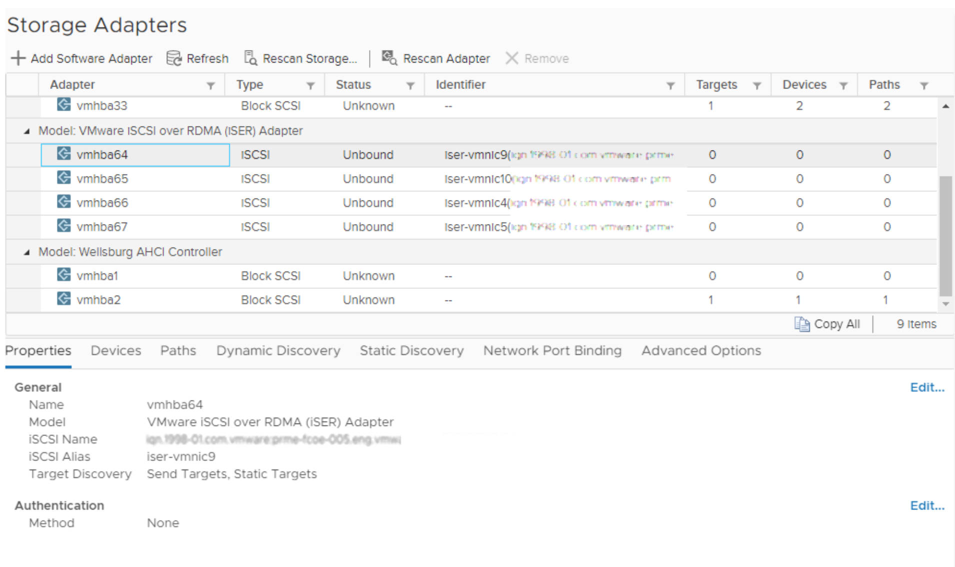
2 Utilice vSphere Client para mostrar el adaptador de iSER.

a En vSphere Client, desplácese hasta el host ESXi.

b Haga clic en la pestaña **Configurar**.

c En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y revise la lista de adaptadores.

Si habilitó el adaptador, se mostrará como un adaptador `vmhba#` de almacenamiento en la lista de la categoría Adaptador de iSCSI de VMware a través de RDMA (iSER).



3 Seleccione el `vmhba#` de almacenamiento de iSER para revisar sus propiedades o realice las siguientes tareas.

Opción	Descripción
Configurar el enlace de puerto para el adaptador de almacenamiento de iSER	Debe crear conexiones de red para vincular el adaptador de almacenamiento de iSER `vmhba#` y el adaptador de red compatible con RDMA `vmnic#`. El proceso de configuración de estas conexiones se denomina enlace de puerto. Para obtener información general sobre el enlace de puerto, consulte Configurar la seguridad de red para iSCSI e iSER. Para configurar el enlace de puerto para iSER, consulte Configurar el enlace de puertos de iSCSI o iSER.
Configurar la detección dinámica o estática para el adaptador de almacenamiento de iSER	Para obtener información, consulte Configurar la detección dinámica o estática para iSCSI e iSER en un host ESXi.
Configurar el protocolo de autenticación por desafío mutuo (CHAP) para el adaptador de almacenamiento de iSER	Para obtener información, consulte Configurar CHAP para un adaptador de almacenamiento de iSCSI o iSER.

Pasos siguientes

Para obtener más información, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/79148.

Modificar propiedades generales de los adaptadores de iSCSI o iSER

Es posible modificar el alias y el nombre predeterminados asignados por el host ESXi a los adaptadores de iSCSI o iSER. En el caso de los adaptadores de iSCSI de hardware independientes, también se puede cambiar la configuración IP predeterminada.

Importante Cuando modifique cualquier propiedad predeterminada de los adaptadores, asegúrese de utilizar el formato correcto para los nombres y las direcciones IP.

Requisitos previos

Privilegio necesario: **Host.Configuración.Configuración de partición de almacenamiento**

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione el adaptador (vmhba#) que desea configurar.
4. Haga clic en la pestaña **Propiedades** y en **Editar** en el panel General.
5. (opcional) Modifique las siguientes propiedades generales.

Opción	Descripción
Nombre iSCSI	Nombre único formado según los estándares de iSCSI que identifica al adaptador de iSCSI. Si cambia el nombre, asegúrese de que el nombre que escriba sea universalmente único y tenga el formato correcto. De lo contrario, algunos dispositivos de almacenamiento podrían no reconocer el adaptador de iSCSI.
Alias iSCSI	Nombre alternativo que se utiliza en lugar del nombre iSCSI.

Resultados

Si cambia el nombre iSCSI, este se utilizará en las nuevas sesiones de iSCSI. En las sesiones existentes, la nueva configuración no se utiliza a menos que cierre la sesión y vuelva a iniciarla.

Pasos siguientes

Para saber qué otros pasos de configuración puede realizar para los adaptadores de almacenamiento de iSCSI o iSER, consulte los siguientes temas:

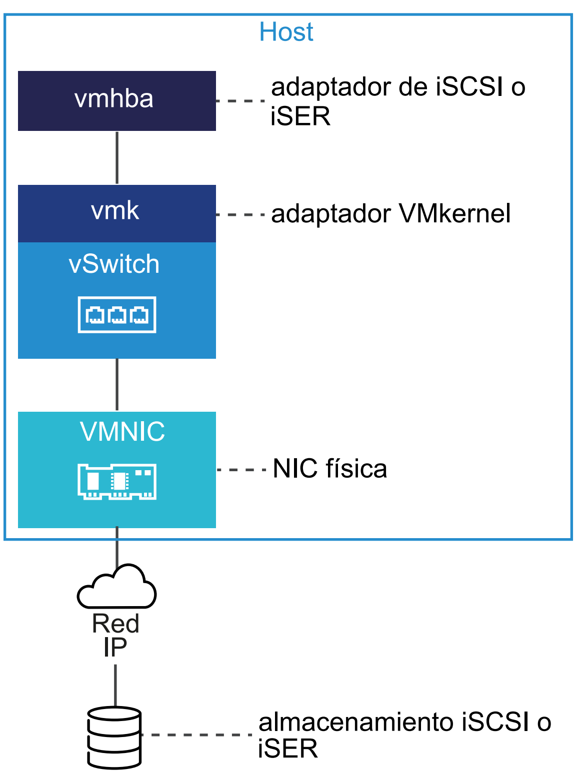
- Configurar adaptadores de iSCSI de hardware independientes

- Configurar los adaptadores de iSCSI de hardware dependiente
- Configurar adaptador de iSCSI de software
- Configurar iSER con ESXi

Configurar la seguridad de red para iSCSI e iSER

Ciertos tipos de adaptadores de iSCSI dependen de las redes de VMkernel. Estos adaptadores incluyen los adaptadores de iSCSI de hardware o de software dependiente y el iSCSI de VMware a través del adaptador RDMA (iSER). Si su entorno incluye alguno de estos adaptadores, debe configurar las conexiones para el tráfico entre el componente de iSCSI o iSER y los adaptadores de red física.

La configuración de la conexión de red implica la creación de un adaptador VMkernel virtual para cada adaptador de red físico. Use una asignación 1:1 entre cada adaptador de red física y virtual. A continuación, asocie el adaptador de VMkernel con un adaptador de iSCSI o iSER adecuado. Este proceso se conoce como enlace de puertos.



Siga estas reglas al configurar el enlace de puertos:

- Puede conectar el adaptador de iSCSI de software con cualquier NIC física disponible en el host.
- Los adaptadores de iSCSI dependientes deben estar conectados solo a sus propias NIC físicas.
- Debe conectar el adaptador de iSER solo con el adaptador de red compatible con RDMA.

Para observar las consideraciones específicas sobre cuándo y cómo utilizar las conexiones de red con iSCSI de software, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2038869.

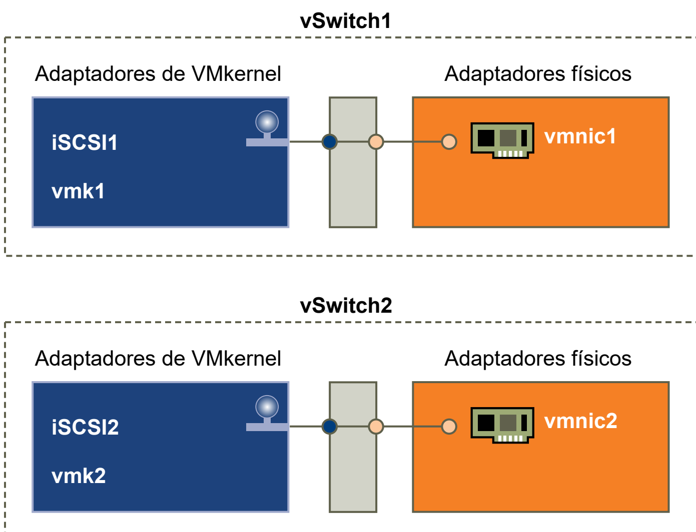
Varios adaptadores de red en la configuración de iSCSI o iSER

Si el host tiene más de un adaptador de red física para iSCSI o iSER, puede utilizar los adaptadores para múltiples rutas.

Puede utilizar varios adaptadores físicos en una configuración de conmutador único o de múltiples conmutadores.

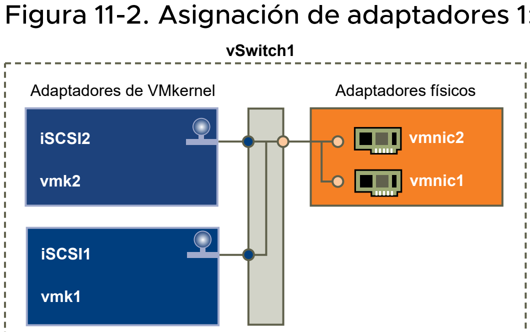
En una configuración de múltiples conmutadores, designe un conmutador de vSphere distinto para cada par de adaptadores virtuales a físicos.

Figura 11-1. Asignación de adaptadores 1:1 en conmutadores estándar de vSphere distintos



Una alternativa es agregar todas las NIC y los adaptadores de VMkernel a un solo conmutador de vSphere. La cantidad de adaptadores de VMkernel debe ser igual a la cantidad de adaptadores físicos en el conmutador estándar de vSphere. La configuración de conmutador único no es adecuada para iSER, ya que iSER no es compatible con la formación de equipos de NIC.

Figura 11-2. Asignación de adaptadores 1:1 en un conmutador estándar de vSphere



Para ese tipo de configuración, se debe anular la configuración de red predeterminada y comprobar que cada adaptador de VMkernel se asigne a solo un adaptador físico activo correspondiente, tal como indica la tabla.

Adaptador VMkernel (vmk#)	Adaptador de red físico (vmnic#)
vmk1 (iSCSI1)	**Adaptadores activos** vmnic 1 **Adaptadores sin utilizar** vmnic 2
vmk2 (iSCSI2)	**Adaptadores activos** vmnic 2 **Adaptadores sin utilizar** vmnic 1

También puede utilizar conmutadores distribuidos. Para obtener más información sobre las instancias de vSphere Distributed Switch y sobre cómo cambiar la directiva de red predeterminada, consulte la documentación de *Redes de vSphere*.

Las siguientes consideraciones se aplican cuando se utilizan varios adaptadores físicos:

- Los adaptadores de red física deben estar en la misma subred que el sistema de almacenamiento al que se conectan.
- (Se aplica solo a iSCSI, no a iSER). Si usa conmutadores de vSphere distintos, debe conectarlos a distintas subredes IP. De lo contrario, es posible que los adaptadores de VMkernel experimenten problemas de conectividad y que el host no detecte los LUN.
- La configuración de conmutador único no es adecuada para iSER, ya que iSER no es compatible con la formación de equipos de NIC.

No utilice enlace de puertos ante cualquiera de las siguientes condiciones:

- Los puertos iSCSI del destino de matriz están en un dominio de difusión y subred IP diferente.
- Los adaptadores VMkernel utilizados para la conectividad iSCSI existen en diferentes dominios de difusión, subredes IP o utilizan conmutadores virtuales distintos.

  Nota En las configuraciones de iSER, los adaptadores de VMkernel utilizados para la conectividad de iSER no pueden utilizarse para tráfico convergente. Los adaptadores de VMkernel que creó para habilitar la conectividad entre el host ESXi con iSER y el destino de iSER deben utilizarse solo para tráfico de iSER.

Prácticas recomendadas para configurar redes con iSCSI de software

Al configurar redes con iSCSI de software, tenga en cuenta las distintas prácticas recomendadas.

Enlace de puertos iSCSI de software

Puede enlazar el iniciador de iSCSI de software en el host ESXi con un único o varios puertos de VMkernel, de modo que el tráfico de iSCSI circule solamente mediante los puertos enlazados. Para el tráfico iSCSI no se utilizan puertos sin enlazar.

Cuando se configura el enlace de puertos, el iniciador de iSCSI crea sesiones iSCSI desde todos los puertos enlazados hasta todos los portales de destino configurados.

Vea los siguientes ejemplos.

Puertos de VMkernel	Portales de destino	Sesiones iSCSI
2 puertos de VMkernel enlazados	2 portales de destino	4 sesiones (2 x 2)
4 puertos de VMkernel enlazados	1 portal de destino	4 sesiones (4 x 1)
2 puertos de VMkernel enlazados	4 portales de destino	8 sesiones (2 x 4)

Nota Al utilizar el enlace de puertos, asegúrese de que todos los portales de destino sean accesibles desde todos los puertos de VMkernel. De lo contrario, es posible que las sesiones iSCSI no puedan crearse. Como resultado, puede que la operación de reexaminación demore más de lo esperado.

Sin enlace de puertos

Si no usa el enlace de puertos, la capa de redes de ESXi selecciona el mejor puerto de VMkernel en función de su tabla de enrutamiento. El host usa el puerto para crear una sesión iSCSI en el portal de destino. Sin el enlace de puertos, solo se crea una sesión por cada portal de destino.

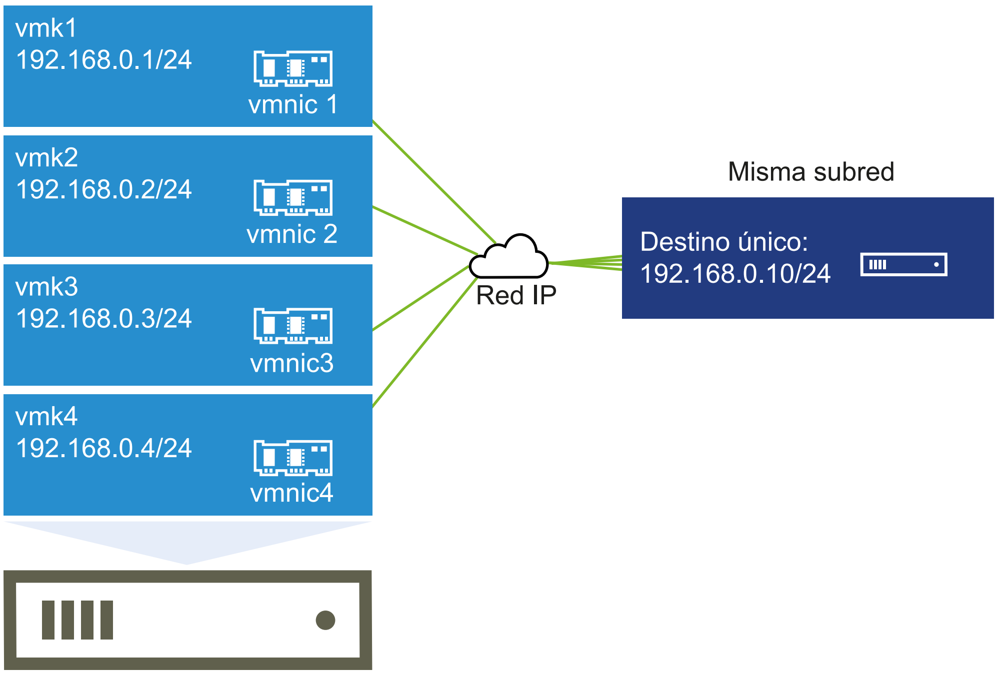
Vea los siguientes ejemplos.

Puertos de VMkernel	Portales de destino	Sesiones iSCSI
2 puertos de VMkernel no enlazados	2 portales de destino	2 sesiones
4 puertos de VMkernel no enlazados	1 portal de destino	1 sesión
2 puertos de VMkernel no enlazados	4 portales de destino	4 sesiones

Creación de múltiples rutas de iSCSI de software

Ejemplo 1. Múltiples rutas para un destino iSCSI con un solo portal de red

Si el destino tiene un solo portal de red, puede crear múltiples rutas para él agregando varios puertos de VMkernel al host ESXi y enlazándolos al iniciador de iSCSI.

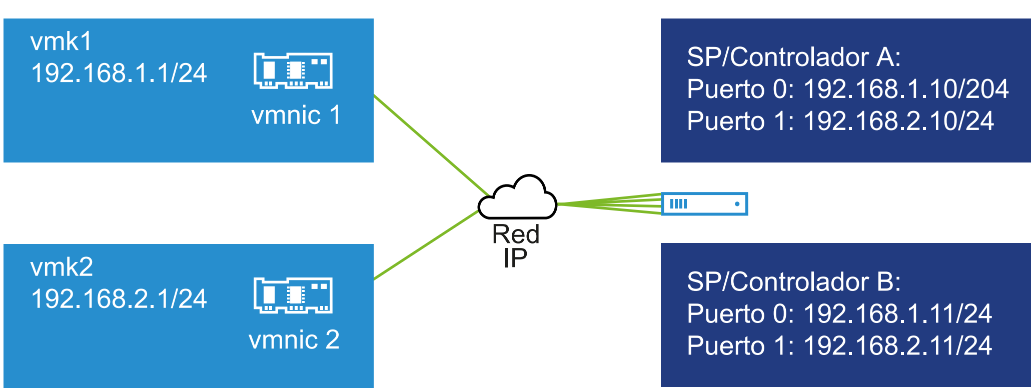


En este ejemplo, todos los puertos de iniciador y el portal de destino están configurados en la misma subred. Es posible acceder al destino mediante todos los puertos enlazados. Cuenta con cuatro puertos de VMkernel y un portal de destino, por lo cual se crea un total de cuatro rutas de acceso.

Sin el enlace de puertos, se crea una sola ruta de acceso.

Ejemplo 2. Múltiples rutas con puertos de VMkernel en diferentes subredes

Puede crear múltiples rutas configurando varios puertos y portales de destino en diferentes subredes IP. Si se mantiene el iniciador y los puertos de destino en diferentes subredes, puede hacer que ESXi cree rutas de acceso mediante puertos específicos. El enlace de puertos no se usa en esta configuración, ya que esto requiere que todos los puertos del iniciador y de destino se encuentren en la misma subred.



ESXi selecciona vmk1 durante la conexión con el puerto 0 del controlador A y controlador B, ya que los tres puertos se encuentran en la misma subred. De modo similar, se selecciona vmk2 durante la conexión con el puerto 1 del controlador A y controlador B. Puede usar la formación de equipos de NIC en esta configuración.

Se crea un total de cuatro rutas de acceso.

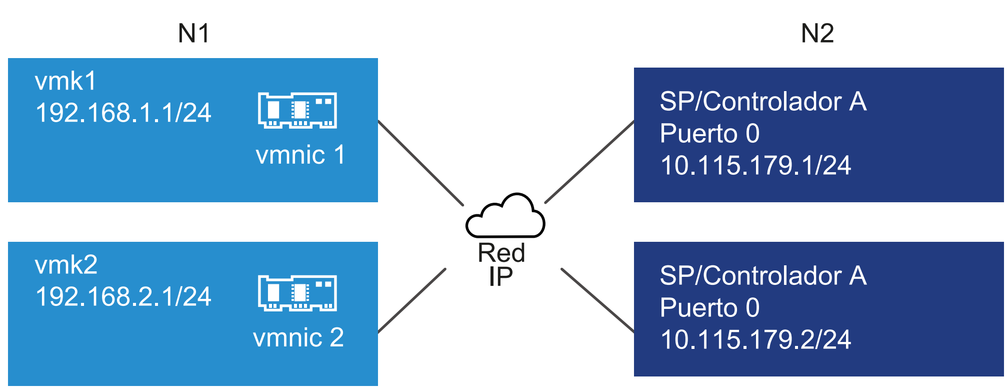
Rutas de acceso	Descripción
Ruta de acceso 1	vmk1 y puerto 0 del controlador A
Ruta de acceso 2	vmk1 y puerto 0 del controlador B
Ruta de acceso 3	vmk2 y puerto 1 del controlador A
Ruta de acceso 4	vmk2 y puerto 1 del controlador B

Enrutamiento con iSCSI de software

Puede usar el comando `esxcli` si desea agregar rutas estáticas para el tráfico de iSCSI. Una vez configuradas las rutas estáticas, los puertos de iniciador y de destino en diferentes subredes pueden comunicarse entre sí.

Ejemplo 1. Uso de rutas estáticas con enlace de puertos

En este ejemplo se conservan todos los puertos de VMkernel enlazados en una subred (N1) y se configuran todos los portales de destino en otra subred (N2). A continuación, se puede agregar una ruta estática para la subred de destino (N2).

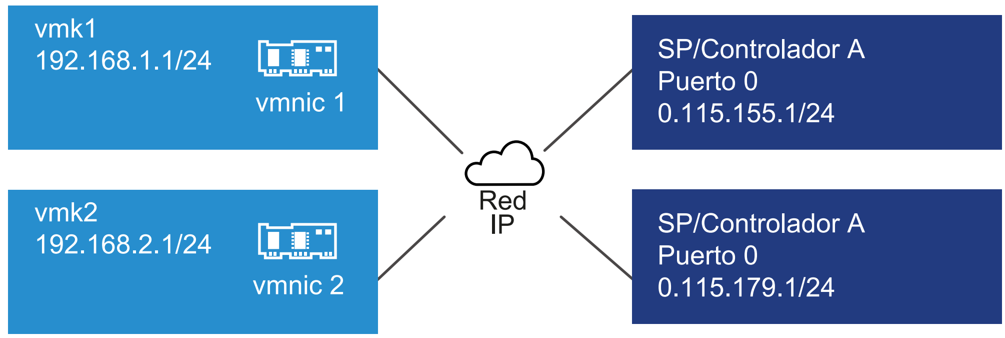


Utilice el siguiente comando:

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network
10.115.179.0/24
```

Ejemplo 2. Uso de rutas estáticas para crear múltiples rutas

En esta configuración, se usan rutas estáticas cuando hay diferentes subredes. No puede usar el enlace de puertos con esta configuración.



Se configuran vmk1 y vmk2 en distintas subredes (192.168.1.0 y 192.168.2.0). Los portales de destino también se encuentran en diferentes subredes (10.115.155.0 y 10.155.179.0).

Puede agregar la ruta estática para 10.115.155.0 desde vmk1. Asegúrese de que pueda accederse a la puerta de enlace desde vmk1.

esxcli network ip route ipv4 add -gateway 192.168.1.253 -network 10.115.155.0/24

A continuación, puede agregar la ruta estática para 10.115.179.0 desde vmk2. Asegúrese de que pueda accederse a la puerta de enlace desde vmk2.

esxcli network ip route ipv4 add -gateway 192.168.2.253 -network 10.115.179.0/24

Durante la conexión con el puerto 0 del controlador A, se usa vmk1.

Durante la conexión con el puerto 0 del controlador B, se usa vmk2.

Ejemplo 3. Enrutamiento con una puerta de enlace distinta por puerto de VMkernel

A partir de vSphere 6.5, se puede configurar una puerta de enlace distinta por cada puerto de VMkernel. Si usa DHCP para obtener la configuración de IP de un puerto de VMkernel, la información de la puerta de enlace también puede obtenerse mediante DHCP.

Para ver la información de la puerta de enlace por cada puerto de VMkernel, utilice el siguiente comando:

esxcli network ip interface ipv4 address list

```
Name  IPv4 Address    IPv4 Netmask   IPv4 Broadcast  Address Type  Gateway         DHCP DNS
----  --------------  -------------  --------------  ------------  --------------  --------
vmk0  10.115.155.122  255.255.252.0  10.115.155.255  DHCP          10.115.155.253      true
vmk1  10.115.179.209  255.255.252.0  10.115.179.255  DHCP          10.115.179.253      true
vmk2  10.115.179.146  255.255.252.0  10.115.179.255  DHCP          10.115.179.253      true
```

Cuando se usan distintas puertas de enlace por cada puerto de VMkernel, el enlace de puertos permite acceder a destinos en diferentes subredes.

Configurar el enlace de puertos de iSCSI o iSER

El enlace de puertos crea conexiones para el tráfico entre ciertos tipos de adaptadores de iSCSI o iSER y los adaptadores de red físicos.

Los siguientes tipos de adaptadores requieren el enlace de puertos:

- Adaptador de iSCSI de software
- Adaptador de iSCSI de hardware dependiente
- Adaptador de iSCSI por RDMA (iSER) de VMware

Las siguientes tareas analizan la configuración de red con un conmutador estándar de vSphere y un adaptador de red físico único. Si tiene varios adaptadores de red, consulte Varios adaptadores de red en la configuración de iSCSI o iSER.

Nota iSER no es compatible con la agrupación de NIC. Al configurar el enlace de puerto para iSER, use solo un adaptador físico habilitado para RDMA (vmnic#) y un adaptador de VMkernel (vmk#) por cada vSwitch.

También puede usar el conmutador distribuido VMware vSphere® Distributed Switch™ y el conmutador virtual VMware NSX® Virtual Switch™ en la configuración de enlace de puertos. Para obtener información sobre los conmutadores virtuales NSX, consulte la documentación de *VMware NSX Data Center for vSphere*.

Si se utiliza un conmutador distribuido de vSphere con varios puertos de vínculo superior, para el enlace de puertos se debe crear un grupo de puertos distribuidos por separado por cada NIC física. A continuación, establezca la directiva de formación de equipos de forma tal que cada grupo de puertos distribuidos tenga un solo puerto de vínculo superior activo. Para obtener información detallada sobre los conmutadores distribuidos, consulte la documentación de *Redes de vSphere*.

Procedimiento

1 Crear un adaptador de VMkernel único para iSCSI o iSER

   Conecte el VMkernel, que ejecuta servicios para almacenamiento iSCSI, a un adaptador de red físico en el host ESXi. A continuación, puede utilizar el adaptador de VMkernel creado en la configuración de enlace de puerto con los adaptadores iSCSI o iSER.

2 Vincular adaptadores de iSCSI o iSER a adaptadores de VMkernel

   En el host ESXi, vincule un adaptador de iSCSI o iSER con un adaptador de VMkernel.

3 Revisar los detalles de enlace de puerto en el host ESXi

   Revise los detalles de redes del adaptador de VMkernel enlazado al adaptador vmhba de iSCSI o iSER.

Pasos siguientes

Para saber qué otros pasos de configuración puede realizar para los adaptadores de almacenamiento de iSCSI o iSER, consulte los siguientes temas:

- Configurar los adaptadores de iSCSI de hardware dependiente
- Configurar adaptador de iSCSI de software
- Configurar iSER con ESXi

Crear un adaptador de VMkernel único para iSCSI o iSER

Conecte el VMkernel, que ejecuta servicios para almacenamiento iSCSI, a un adaptador de red físico en el host ESXi. A continuación, puede utilizar el adaptador de VMkernel creado en la configuración de enlace de puerto con los adaptadores iSCSI o iSER.

Los siguientes tipos de adaptadores requieren el enlace de puertos:

- Adaptador de iSCSI de software
- Adaptador de iSCSI de hardware dependiente
- Adaptador de iSCSI por RDMA (iSER) de VMware

Requisitos previos

- Si crea un adaptador de VMkernel para iSCSI hardware dependiente, debe seleccionar el adaptador de red físico (vmnic#) que corresponda al componente iSCSI. Consulte Determinar la asociación entre iSCSI y los adaptadores de red.
- Para el adaptador de iSER, asegúrese de utilizar una vmnic# adecuada compatible con RDMA. Consulte Instalar y ver un adaptador de red compatible con RDMA.

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. En el menú contextual, seleccione **Agregar redes**.
3. Seleccione **Adaptador de red de VMkernel** y haga clic en **Siguiente**.
4. Seleccione **Nuevo conmutador estándar** para crear un conmutador de vSphere Standard.
5. Haga clic en el icono **Agregar adaptadores** y seleccione el adaptador de red (vmnic#) adecuado para utilizarlo en iSCSI.

   Asegúrese de asignar el adaptador a Adaptadores activos.
6. Introduzca una etiqueta de red.

   Una etiqueta de red es un nombre descriptivo que identifica al adaptador de VMkernel que se está creando, por ejemplo, iSCSI o iSER.
7. Especifique la configuración IP.

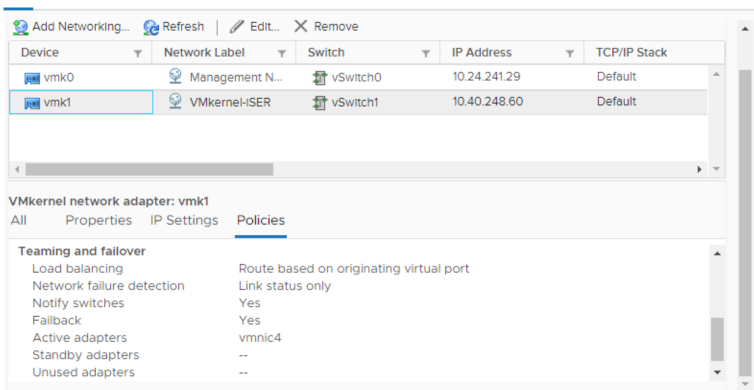
8 Revise la información y haga clic en **Finalizar**.

   Creó el adaptador VMkernel virtual (vmk#) para un adaptador de red física (vmnic#) en el host.

9 Compruebe su configuración.

   a En **Redes**, seleccione **Adaptadores de VMkernel** y seleccione el adaptador de VMkernel (vmk#) de la lista.

   b Haga clic en la pestaña **Directivas** y compruebe que el adaptador de red físico (vmnic#) correspondiente aparece como un adaptador activo en **Formación de equipos y conmutación por error**.



Pasos siguientes

Si el host tiene un adaptador de red físico para tráfico iSCSI, enlace el adaptador de VMkernel que creó con el adaptador vmhba de iSCSI o iSER.

Si tiene varios adaptadores de red, puede crear adaptadores de VMkernel adicionales y, a continuación, realice el enlace de iSCSI. La cantidad de adaptadores virtuales debe ser igual a la cantidad de adaptadores físicos del host. Para obtener información, consulte Varios adaptadores de red en la configuración de iSCSI o iSER.

Vincular adaptadores de iSCSI o iSER a adaptadores de VMkernel

En el host ESXi, vincule un adaptador de iSCSI o iSER con un adaptador de VMkernel.

Los siguientes tipos de adaptadores requieren el enlace de puertos:

- Adaptador de iSCSI de software
- Adaptador de iSCSI de hardware dependiente
- Adaptador de iSCSI por RDMA (iSER) de VMware

Requisitos previos

Cree un adaptador VMkernel virtual para cada adaptador de red físico del host. Si utiliza varios adaptadores VMkernel, configure la directiva de red correcta.

Privilegio necesario: **Host.Configuración.Configuración de partición de almacenamiento**

Procedimiento

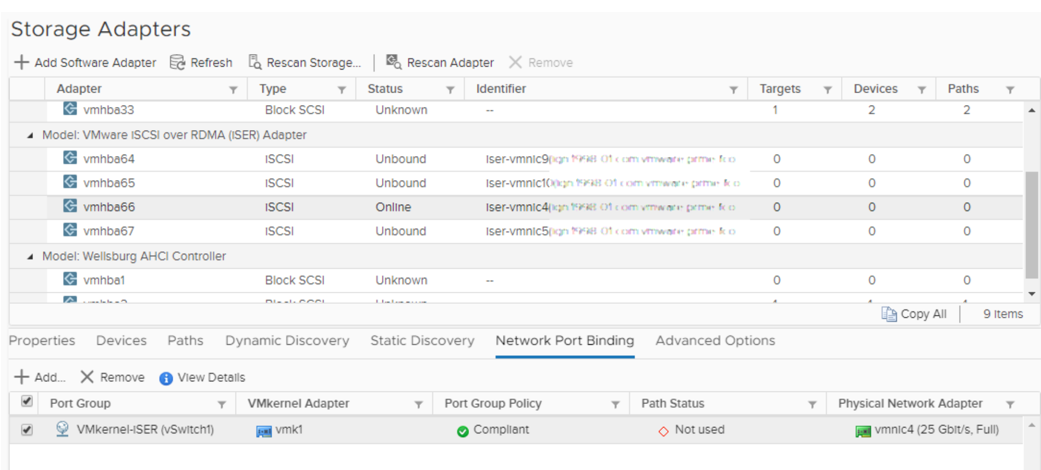
1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione el adaptador de iSCSI o iSER (vmhba#) adecuado en la lista.
4. Haga clic en la pestaña **Enlace de puertos de red** y en el icono **Agregar**.
5. Seleccione un adaptador de VMkernel para vincular con el adaptador de iSCSI o iSER.

   Nota Asegúrese de que la directiva de red del adaptador VMkernel cumpla con los requisitos de unión.

   Se puede vincular el adaptador de iSCSI de software con uno o más adaptadores VMkernel. En el caso de un adaptador de iSCSI de hardware dependiente o el adaptador de iSER, solo hay disponible un adaptador de VMkernel asociado con la NIC física correcta.

6. Haga clic en **Aceptar**.

   La conexión de red aparece en la lista de enlaces de puerto de red para el adaptador de iSCSI o iSER.



Revisar los detalles de enlace de puerto en el host ESXi

Revise los detalles de redes del adaptador de VMkernel enlazado al adaptador vmhba de iSCSI o iSER.

Los siguientes tipos de adaptadores requieren el enlace de puertos:

- Adaptador de iSCSI de software
- Adaptador de iSCSI de hardware dependiente
- Adaptador de iSCSI por RDMA (iSER) de VMware

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.
2 Haga clic en la pestaña **Configurar**.
3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione el adaptador de iSCSI o iSER adecuado en la lista.
4 Haga clic en la pestaña **Enlace de puertos de red** y seleccione el adaptador de VMkernel de la lista.
5 Haga clic en el icono **Ver detalles**.
6 Revise la información sobre el adaptador de VMkernel y el adaptador físico alternando entre las pestañas disponibles.

Administrar una red iSCSI

Se aplican consideraciones especiales a adaptadores de red, tanto físicos como VMkernel, que están asociados con un adaptador de iSCSI.

Después de crear conexiones de red para iSCSI, se habilita un indicador de iSCSI en vSphere Client. El indicador muestra que un adaptador de red virtual o físico está enlazado con iSCSI. Para evitar interrupciones en el tráfico iSCSI, siga estas instrucciones y consideraciones al administrar adaptadores de red virtuales y físicos enlazados con iSCSI:

- Asegúrese de que los adaptadores de red del VMkernel tengan asignadas direcciones en la misma subred que el portal de almacenamiento iSCSI al que se conectan.
- Los adaptadores de iSCSI que usan adaptadores de VMkernel no pueden conectarse a puertos iSCSI en subredes diferentes, incluso si los adaptadores de iSCSI detectan esos puertos.
- Al usar conmutadores vSphere individuales para conectar adaptadores de red físicos y adaptadores VMkernel, asegúrese de que los conmutadores vSphere se conecten con subredes de diferente IP.
- Si los adaptadores VMkernel están en la misma subred, deben conectarse a un solo vSwitch.
- Si migra adaptadores VMkernel a un conmutador de vSphere diferente, mueva los adaptadores físicos asociados.
- No cambie la configuración de los adaptadores VMkernel o los adaptadores de red físicos enlazados con iSCSI.
- No realice cambios que puedan romper la asociación de adaptadores VMkernel y adaptadores de red físicos. Si elimina uno de los adaptadores o el conmutador de vSphere que los conecta, puede romper la asociación. Esto también puede ocurrir si cambia la directiva de red 1:1 para su conexión.

Solucionar problemas de red de iSCSI

Un cartel de advertencia indica que una directiva de grupo de puertos no cumple con los requisitos de un adaptador VMkernel enlazado con iSCSI.

Problema

Se considera que la directiva de grupo de puertos del adaptador VMkernel no cumple con los requisitos en los casos siguientes:

- El adaptador VMkernel no está conectado a un adaptador de red físico activo.
- El adaptador VMkernel está conectado a más de un adaptador de red físico.
- El adaptador VMkernel está conectado a uno o más adaptadores físicos en espera.
- Se cambia el adaptador físico activo.

Solución

Configure la directiva de red correcta para el adaptador de VMkernel enlazado con iSCSI. Consulte Configurar la seguridad de red para iSCSI e iSER.

Usar tramas gigantes con iSCSI y con iSER

ESXi admite la utilización de tramas gigantes con iSCSI y con iSER.

Las tramas gigantes son tramas Ethernet con un tamaño superior a 1.500 bytes. El parámetro de unidad de transmisión máxima (MTU) generalmente se utiliza para medir el tamaño de las tramas gigantes.

Cuando se utilizan tramas gigantes para el tráfico iSCSI, aplican las consideraciones siguientes:

- Todos los componentes de red deben admitir tramas gigantes.
- Consulte con los proveedores para asegurarse de que las NIC físicas y los adaptadores de iSCSI sean compatibles con tramas gigantes.
- Para configurar y comprobar conmutadores de red físicos para tramas gigantes, consulte la documentación del proveedor.

La tabla siguiente explica el nivel de compatibilidad que proporciona ESXi para las tramas gigantes.

Tabla 11-1. Compatibilidad con tramas gigantes

Tipo de adaptadores de iSCSI	Compatibilidad con tramas gigantes
iSCSI de software	Compatible
iSCSI de hardware dependiente	Compatible. Compruebe con el proveedor.
iSCSI de hardware independiente	Compatible. Compruebe con el proveedor.
iSER de VMware	Compatible. Compruebe con el proveedor.

Habilitar tramas gigantes para redes

Puede habilitar las tramas gigantes para los adaptadores de almacenamiento ESXi que usan redes VMkernel para su tráfico. Estos adaptadores incluyen adaptadores de iSCSI de software, adaptadores de iSCSI de hardware dependiente y adaptadores de iSER de VMware.

Para habilitar las tramas gigantes, cambie el valor predeterminado del parámetro MTU. Puede cambiar el parámetro MTU en el conmutador de vSphere que usa para el tráfico iSCSI. Para obtener más información, consulte la documentación sobre *Redes de vSphere*.

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Redes**, haga clic en **Conmutadores virtuales** y, desde la lista, seleccione el conmutador de vSphere que desea modificar.
4. Haga clic en el icono **Editar configuración**.
5. En la página Propiedades, cambie el parámetro MTU.

   Este paso establece la MTU para todas las NIC físicas en ese conmutador estándar. Establezca el valor de MTU con el tamaño de MTU más grande entre todas las NIC conectadas al conmutador estándar. ESXi admite un tamaño máximo de MTU de 9.000 bytes.

Habilitar tramas gigantes para iSCSI de hardware independiente

Para habilitar tramas gigantes para adaptadores de iSCSI de hardware independiente en el host ESXi, cambie el valor predeterminado del parámetro de unidades de transmisión máximas (Maximum Transmission Units, MTU).

Utilice la configuración de Opciones avanzadas para cambiar el parámetro MTU en el HBA iSCSI.

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione el adaptador de iSCSI de hardware independiente de la lista de adaptadores.
4. Haga clic en la pestaña **Opciones avanzadas** y seleccione **Editar**.
5. Cambie el valor del parámetro MTU.

   ESXi admite un tamaño máximo de 9.000 bytes para MTU.

Configurar la detección dinámica o estática para iSCSI e iSER en un host ESXi

Se deben configurar direcciones de detección de destino, para que el adaptador de almacenamiento de iSCSI o iSER pueda determinar qué recurso de almacenamiento de la red está disponible para el acceso.

El sistema ESXi es compatible con estos métodos de detección:

Detección dinámica

También conocida como detección SendTargets. Cada vez que el iniciador contacta con un servidor iSCSI especificado, el iniciador envía la solicitud de SendTargets al servidor. El servidor responde proporcionando una lista de destinos disponibles al iniciador. Los nombres y las direcciones IP de estos destinos aparecen en la pestaña **Detección estática**. Si se quita un destino estático agregado con la detección dinámica, el destino puede ser devuelto a la lista la próxima vez que se vuelva a examinar, que se restablezca el adaptador de almacenamiento o que se reinicie el host.

Nota Con iSCSI de hardware dependiente y software, ESXi filtra las direcciones de destino según la familia de IP de la dirección del servidor iSCSI especificado. Si la dirección es IPv4, se filtran las direcciones IPv6 que pueden aparecer en la respuesta SendTargets desde el servidor iSCSI y se las excluye. Cuando se utilizan nombres DNS para especificar un servidor iSCSI o cuando la respuesta SendTargets desde el servidor iSCSI tiene nombres DNS, ESXi depende de la familia de IP de la primera entrada resuelta de la búsqueda de DNS.

Detección estática

Además del método de detección dinámica, se puede utilizar una detección estática e introducir manualmente la información de los destinos. El adaptador de iSCSI o iSER utiliza una lista de destinos que se proporcionan para ponerse en contacto y comunicarse con los servidores iSCSI.

Al configurar la detección estática o dinámica, solo se pueden agregar destinos iSCSI nuevos. No se puede cambiar ningún parámetro de un destino existente. Para hacer cambios, quite el destino existente y agregue uno nuevo.

Requisitos previos

Privilegio necesario: **Host.Configuración.Configuración de partición de almacenamiento**

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione el adaptador (vmhba#) que desea configurar.

4 Configure el método de detección.

Método de detección	Descripción
Detección dinámica	a Haga clic en **Detección dinámica** y, a continuación, en **Agregar**. b Escriba la dirección IP o el nombre DNS del sistema de almacenamiento y haga clic en **Aceptar**. c Vuelva a examinar el adaptador de iSCSI. Después de establecer la sesión de SendTargets con el sistema iSCSI, el host rellena la lista de detección estática con todos los destinos recién detectados. **Nota** Un destino detectado dinámicamente permanece en la lista incluso después de quitarlo del lado de la matriz.
Detección estática	a Haga clic en **Detección estática** y, a continuación, en **Agregar**. b Introduzca la información del destino y haga clic en **Aceptar**. c Vuelva a examinar el adaptador de iSCSI.

Pasos siguientes

Para saber qué otros pasos de configuración puede realizar para los adaptadores de almacenamiento de iSCSI o iSER, consulte los siguientes temas:

- Configurar adaptadores de iSCSI de hardware independientes
- Configurar los adaptadores de iSCSI de hardware dependiente
- Configurar adaptador de iSCSI de software
- Configurar iSER con ESXi

Quitar destinos iSCSI dinámicos o estáticos

Elimine los servidores iSCSI conectados al host ESXi.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione en la lista el adaptador de iSCSI que desea modificar.

4 Cambie entre **Detección dinámica** y **Detección estática**.

5 Seleccione el servidor iSCSI que desea quitar y haga clic en **Quitar**.

6 Vuelva a examinar el adaptador de iSCSI.

Si va a quitar el destino estático que se detectó de forma dinámica, debe quitarlo del sistema de almacenamiento antes de volver a examinar. De lo contrario, el host detecta y agrega automáticamente el destino a la lista de destinos estáticos cuando se vuelva a examinar el adaptador.

Configurar los parámetros de CHAP para los adaptadores de almacenamiento de iSCSI o iSER

Dado que las redes IP que utiliza la tecnología iSCSI para conectarse a destinos remotos no protege los datos que transporta, se debe garantizar la seguridad de la conexión. Uno de los protocolos que iSCSI implementa es el protocolo Challenge Handshake Authentication Protocol (CHAP), que comprueba la legitimidad de los iniciadores que acceden a los destinos en la red.

CHAP utiliza un algoritmo de enlace triple para comprobar la identidad del host y, si corresponde, del destino iSCSI cuando el host y el destino establecen una conexión. La comprobación se basa en un valor privado predefinido, o un secreto CHAP, que comparten el iniciador y el destino.

ESXi admite la autenticación de CHAP en el nivel del adaptador. En este caso, todos los destinos reciben el mismo nombre y el mismo secreto CHAP por parte del iniciador iSCSI. En el caso de los adaptadores de iSCSI de software y de hardware dependiente, así como los adaptadores de iSER, ESXi también admite la autenticación de CHAP por destino, que permite configurar distintas credenciales para cada destino para lograr un nivel de mayor de seguridad.

Selección del método de autenticación de CHAP

ESXi admite CHAP unidireccional para todos los tipos de iniciadores iSCSI/iSER, y CHAP bidireccional para iSCSI de software y hardware dependiente, así como para iSER.

Antes de configurar CHAP, compruebe si CHAP está habilitado en el sistema de almacenamiento iSCSI. Además, averigüe cuál es el método de autenticación de CHAP compatible con el sistema. Si CHAP está habilitado, configúrelo para los iniciadores y asegúrese de que las credenciales de autenticación de CHAP coincidan con las credenciales en el almacenamiento iSCSI.

ESXi admite los siguientes métodos de autenticación de CHAP:

CHAP unidireccional

En la autenticación de CHAP unidireccional, el destino autentica el iniciador, pero el iniciador no autentica el destino.

CHAP bidireccional

La autenticación de CHAP bidireccional aporta un nivel adicional de seguridad. Con este método, el iniciador puede autenticar también el destino. VMware admite este método para adaptadores de iSCSI de software y de hardware dependiente, así como para adaptadores de iSER.

Para adaptadores de iSCSI de software y de hardware dependiente, así como para adaptadores de iSER, se puede establecer CHAP unidireccional y CHAP bidireccional para cada adaptador o en el nivel del destino. iSCSI de hardware independiente admite CHAP solo en el nivel del adaptador.

Cuando establezca los parámetros de CHAP, especifique un nivel de seguridad para CHAP.

Nota Cuando se especifica el nivel de seguridad de CHAP, la forma en que responde la matriz de almacenamiento depende de la implementación de CHAP de la matriz, y es específica del proveedor. Para obtener información sobre el comportamiento de la autenticación de CHAP en diferentes configuraciones de iniciador y destino, consulte la documentación de la matriz.

Tabla 11-2. Nivel de seguridad de CHAP

Nivel de seguridad de CHAP	Descripción	Adaptadores de almacenamiento compatibles
Ninguna	El host no utiliza autenticación de CHAP. Si la autenticación está habilitada, utilice esta opción para deshabilitarla.	iSCSI de hardware independiente iSCSI de software iSCSI de hardware dependiente iSER
Usar CHAP unidireccional, si el destino lo requiere	El host prefiere una conexión que no sea CHAP, pero se puede utilizar una conexión CHAP si el destino lo requiere.	iSCSI de software iSCSI de hardware dependiente iSER
Usar CHAP unidireccional, a menos que el destino lo prohíba	El host prefiere CHAP, pero se pueden utilizar conexiones que no sean CHAP si el destino no admite CHAP.	iSCSI de hardware independiente iSCSI de software iSCSI de hardware dependiente iSER
Usar CHAP unidireccional	El host requiere una autenticación de CHAP correcta. La conexión genera un error si falla la negociación de CHAP.	iSCSI de hardware independiente iSCSI de software iSCSI de hardware dependiente iSER
Utilizar CHAP bidireccional	Tanto el host como el destino admiten CHAP bidireccional.	iSCSI de software iSCSI de hardware dependiente iSER

Configurar CHAP para un adaptador de almacenamiento de iSCSI o iSER

Cuando se configura el nombre y el secreto del CHAP en el nivel del adaptador de iSCSI/iSER, todos los destinos reciben los mismos parámetros del adaptador. De forma predeterminada, todas las direcciones de detección o destinos estáticos heredan los parámetros del CHAP configurados en el nivel del adaptador.

El nombre de CHAP no debe superar los 511 caracteres alfanuméricos, mientras que el secreto CHAP no debe superar los 255 caracteres alfanuméricos. Algunos adaptadores, por ejemplo, el adaptador QLogic, pueden tener límites más bajos: 255 caracteres para el nombre de CHAP y 100 para el secreto CHAP.

Requisitos previos

- Antes de configurar los parámetros de CHAP para iSCSI de hardware dependiente o de software, determine si desea configurar CHAP unidireccional o bidireccional. Los adaptadores iSCSI de hardware independiente no admiten CHAP bidireccional.
- Compruebe los parámetros de CHAP configurados en el almacenamiento. Los parámetros configurados deben coincidir con los del almacenamiento.
- Privilegio necesario: **Host.Configuración.Configuración de partición de almacenamiento**

Procedimiento

1 Desplácese hasta el adaptador de almacenamiento de iSCSI o iSER.

   a En vSphere Client, desplácese hasta el host ESXi.

   b Haga clic en la pestaña **Configurar**.

   c En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione el adaptador (vmhba#) que desea configurar.

2 Haga clic en la pestaña **Propiedades** y en la opción **Editar** del panel **Autenticación**.

3 Especifique el método de autenticación.

   - **Ninguno**
   - **Usar CHAP unidireccional, si el destino lo requiere**
   - **Usar CHAP unidireccional, a menos que el destino lo prohíba**
   - **Usar CHAP unidireccional**
   - **Usar CHAP bidireccional**. Para configurar el CHAP bidireccional, debe seleccionar esta opción.

4 Especifique el nombre de CHAP saliente.

   Asegúrese de que el nombre que especifique coincida con el nombre configurado en el lado del almacenamiento.

   - Para establecer el nombre de CHAP con el nombre del adaptador de iSCSI, seleccione **Usar nombre del iniciador**.
   - Para establecer el nombre de CHAP con cualquier otro nombre distinto del nombre del iniciador iSCSI, desactive la casilla **Usar nombre del iniciador** y escriba un nombre en el cuadro de texto **Nombre**.

5 Introduzca el secreto de CHAP saliente que desea utilizar como parte de la autenticación. Utilice la misma contraseña que escribió en el lado del almacenamiento.

6 Si configura CHAP bidireccional, especifique credenciales de CHAP entrantes.

   Asegúrese de utilizar diferentes secretos para el CHAP saliente y entrante.

7 Haga clic en **Aceptar**.

8 Vuelva a examinar el adaptador de iSCSI.

Resultados

Si cambia los parámetros de CHAP, se utilizarán para nuevas sesiones de iSCSI. En las sesiones existentes, la nueva configuración no se utiliza a menos que cierre la sesión y vuelva a iniciarla.

Pasos siguientes

Para saber qué otros pasos de configuración puede realizar para los adaptadores de almacenamiento de iSCSI o iSER, consulte los siguientes temas:

- Configurar adaptadores de iSCSI de hardware independientes
- Configurar los adaptadores de iSCSI de hardware dependiente
- Configurar adaptador de iSCSI de software
- Configurar iSER con ESXi

Configurar CHAP para un destino

Si utiliza adaptadores de iSCSI de hardware dependiente y de software, o un adaptador de almacenamiento de iSER, puede configurar diferentes credenciales CHAP para cada dirección de detección o destino estático.

El nombre de CHAP no debe superar los 511 caracteres alfanuméricos, en tanto que el secreto CHAP no debe superar los 255 caracteres alfanuméricos.

Requisitos previos

- Antes de configurar los parámetros de CHAP, determine si desea configurar CHAP unidireccional o bidireccional.
- Compruebe los parámetros de CHAP configurados en el almacenamiento. Los parámetros configurados deben coincidir con los del almacenamiento.
- Privilegio necesario: **Host.Configuración.Configuración de partición de almacenamiento**

Procedimiento

1 Desplácese hasta el adaptador de almacenamiento de iSCSI o iSER.

   a En vSphere Client, desplácese hasta el host ESXi.

   b Haga clic en la pestaña **Configurar**.

   c En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione el adaptador (vmhba#) que desea configurar.

2 Haga clic en **Detección dinámica** o **Detección estática**.

3 En la lista de destinos disponibles, seleccione el destino que desea configurar y haga clic en **Autenticación**.

4 Anule la selección de **Heredar configuración del primario** y especifique el método de autenticación.

- **Ninguno**
- **Usar CHAP unidireccional, si el destino lo requiere**
- **Usar CHAP unidireccional, a menos que el destino lo prohíba**
- **Usar CHAP unidireccional**
- **Usar CHAP bidireccional**. Para configurar el CHAP bidireccional, debe seleccionar esta opción.

5 Especifique el nombre de CHAP saliente.

Asegúrese de que el nombre que especifique coincida con el nombre configurado en el lado del almacenamiento.

- Para establecer el nombre de CHAP con el nombre del adaptador de iSCSI, seleccione **Usar nombre del iniciador**.
- Para establecer el nombre de CHAP con cualquier otro nombre distinto del nombre del iniciador iSCSI, desactive la casilla **Usar nombre del iniciador** y escriba un nombre en el cuadro de texto **Nombre**.

6 Introduzca el secreto de CHAP saliente que desea utilizar como parte de la autenticación. Utilice la misma contraseña que escribió en el lado del almacenamiento.

7 Si configura CHAP bidireccional, especifique credenciales de CHAP entrantes.

Asegúrese de utilizar diferentes secretos para el CHAP saliente y entrante.

8 Haga clic en **Aceptar**.

9 Vuelva a examinar el adaptador de almacenamiento.

Resultados

Si cambia los parámetros de CHAP, se utilizarán para nuevas sesiones de iSCSI. Para las sesiones actuales, no se utilizará la configuración nueva hasta que cierre la sesión y vuelva a iniciarla.

Configurar los parámetros avanzados de iSCSI

Es posible que deba configurar parámetros adicionales para los iniciadores iSCSI en el host ESXi. Por ejemplo, algunos sistemas de almacenamiento iSCSI requieren una redirección a través del protocolo Address Resolution Protocol (ARP) para mover de manera dinámica el tráfico iSCSI de un puerto a otro. En este caso, debe activar la redirección de ARP en el host.

En la siguiente tabla, se enumeran los parámetros avanzados de iSCSI que se pueden configurar con vSphere Client. Además, se pueden utilizar los comandos de la CLI de vSphere para configurar algunos de los parámetros avanzados. Para obtener información, consulte el documento *Introducción a ESXCLI*.

Según el tipo de adaptadores, es posible que algunos parámetros no estén disponibles.

Importante No cambie la configuración avanzada de iSCSI, a menos que el soporte de VMware o los proveedores de almacenamiento le indiquen que la cambie.

Tabla 11-3. Parámetros adicionales de los iniciadores iSCSI

Parámetro avanzado	Descripción
Resumen de encabezados	Aumenta la integridad de los datos. Cuando se habilita el parámetro de resumen de encabezados, el sistema realiza una suma de comprobación en cada parte del encabezado de la unidad de datos de protocolo (PDU) de iSCSI. El sistema comprueba los datos con el algoritmo CRC32C.
Resumen de datos	Aumenta la integridad de los datos. Cuando se habilita el parámetro de resumen de datos, el sistema realiza una suma de comprobación sobre cada parte de los datos de la PDU. El sistema comprueba los datos con el algoritmo CRC32C. **Nota** Los sistemas que utilizan los procesadores Intel Nehalem descargan los cálculos del resumen de iSCSI para iSCSI de software. Esta descarga sirve para ayudar a reducir el impacto sobre el rendimiento.
ErrorRecoveryLevel	Valor del nivel de recuperación de errores (Error Recovery Level, ERL) de iSCSI que el iniciador iSCSI del host negocia durante el inicio de sesión.
LoginRetryMax	Cantidad máxima de veces que el iniciador iSCSI de ESXi intenta iniciar sesión en un destino antes de finalizar los intentos.
MaxOutstandingR2T	Define las PDU listas para la transferencia (R2T) que pueden estar en transición antes de recibir una PDU de reconocimiento.
FirstBurstLength	Especifica la cantidad máxima de datos no solicitados que un iniciador iSCSI puede enviar al destino durante la ejecución de un solo comando SCSI, en bytes.
MaxBurstLength	Carga útil de datos de SCSI máxima en una secuencia de iSCSI de entrada de datos o de salida de datos solicitada, en bytes.
MaxRecvDataSegLength	Longitud máxima del segmento de datos, en bytes, que puede recibirse en una PDU de iSCSI.
MaxCommands	Comandos de SCSI máximos que pueden estar en cola en el adaptador de iSCSI.
DefaultTimeToWait	Tiempo mínimo en segundos que se debe esperar para intentar cerrar sesión o reasignar una tarea activa después de la finalización o del restablecimiento inesperado de la conexión.
DefautTimeToRetain	Tiempo máximo en segundos durante el cual la reasignación de la tarea activa aún es posible después de la finalización o del restablecimiento de la conexión.
LoginTimeout	Tiempo en segundos que el iniciador espera para que finalice la respuesta de inicio de sesión.
LogoutTimeout	Tiempo en segundos que el iniciador espera para obtener una respuesta de la PDU de solicitud de cierre de sesión.

Tabla 11-3. Parámetros adicionales de los iniciadores iSCSI (continuación)

Parámetro avanzado	Descripción
RecoveryTimeout	Especifica la cantidad de tiempo, en segundos, que puede transcurrir mientras se recupera una sesión. Si el tiempo de espera supera el límite, el iniciador iSCSI finaliza la sesión.
Intervalo de No-Op	Especifica el intervalo, en segundos, entre las solicitudes de NOP-Out enviadas del iniciador iSCSI a un destino iSCSI. Las solicitudes NOP-Out actúan como el mecanismo de ping para comprobar que existe una conexión activa entre el iniciador iSCSI y el destino iSCSI.
Tiempo de espera de No-Op	Especifica la cantidad de tiempo, en segundos, que puede transcurrir antes de que el host reciba un mensaje de NOP-In. El destino iSCSI envía el mensaje en respuesta a la solicitud NOP-Out. Cuando se supera el límite del tiempo de espera de no-op, el iniciador finaliza la sesión actual y comienza una nueva.
Redirección de ARP	Con este parámetro habilitado, los sistemas de almacenamiento pueden mover el tráfico iSCSI dinámicamente desde un puerto a otro. Los sistemas de almacenamiento que realizan conmutaciones por error basadas en matrices requieren el parámetro ARP.
ACK demorado	Con este parámetro habilitado, los sistemas de almacenamiento pueden retrasar una confirmación de los paquetes de datos recibidos.

Configurar parámetros avanzados para iSCSI en el host ESXi

La configuración avanzada de iSCSI controla los parámetros, como el encabezado y el resumen de datos, la redirección de ARP, ACK demorado, etc.

Precaución No haga cambios en la configuración de iSCSI avanzada a menos que esté trabajando con el equipo de soporte de VMware o que tenga información detallada sobre los valores que debe asignar a la configuración.

Requisitos previos

Privilegio necesario: **Host.Configuración.Configuración de partición de almacenamiento**

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione el adaptador (vmhba#) que desea configurar.

4 Configure los parámetros avanzados.

Opción	Descripción
En el nivel del adaptador	Haga clic en la pestaña **Opciones avanzadas** y seleccione **Editar**.
n el nivel del destino	a Haga clic en **Detección dinámica** o **Detección estática**. b En la lista de destinos disponibles, seleccione el destino que desea configurar y haga clic en **Avanzado**.

5 Introduzca todos los valores requeridos de los parámetros avanzados que desea modificar.

Administrar sesiones de iSCSI

Para comunicarse entre sí, los iniciadores iSCSI y los destinos establecen sesiones iSCSI. Puede revisar y administrar las sesiones iSCSI con vSphere CLI.

De forma predeterminada, los iniciadores iSCSI de hardware dependiente e iSCSI de software inician una sesión iSCSI entre cada puerto del iniciador y cada puerto de destino. Si el iniciador iSCSI o el destino tienen más de un puerto, se pueden establecer varias sesiones en el host. La cantidad predeterminada de sesiones para cada destino equivale a la cantidad de puertos en el adaptador de iSCSI multiplicada por la cantidad de puertos de destino.

Con vSphere CLI, puede mostrar todas las sesiones actuales para analizarlas y depurarlas. Para crear más rutas de acceso a los sistemas de almacenamiento, puede aumentar la cantidad predeterminada de sesiones duplicando las sesiones existentes entre el adaptador de iSCSI y los puertos de destino.

También puede establecer una sesión con un puerto de destino específico. Esta capacidad resulta muy útil si el host se conecta a un sistema de almacenamiento de un solo puerto que presenta solo un puerto de destino al iniciador. El sistema redirecciona entonces las sesiones adicionales a otro puerto de destino. Establecer una sesión nueva entre el iniciador iSCSI y otro puerto de destino crea una ruta de acceso adicional al sistema de almacenamiento.

Las consideraciones siguientes aplican a la administración de sesión de iSCSI:

- Algunos sistemas de almacenamiento no admiten varias sesiones del mismo extremo o nombre de iniciador. Los intentos de crear varias sesiones en tales destinos puede resultar en un comportamiento impredecible de su entorno iSCSI.
- Los proveedores de almacenamiento pueden proporcionar administradores de sesión automáticos. Utilizar los administradores de sesión automáticos para agregar o eliminar sesiones no garantiza resultados duraderos y puede interferir con el rendimiento del almacenamiento.

Revisar las sesiones iSCSI

Utilice el comando vCLI para mostrar sesiones iSCSI entre un adaptador de iSCSI y un sistema de almacenamiento.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

- ◆ Para enumerar las sesiones iSCSI, ejecute el siguiente comando:

  `esxcli iscsi session list`

Este comando toma estas opciones:

Opción	Descripción
-A|--adapter=*str*	El nombre del adaptador de iSCSI, por ejemplo, vmhba34.
-s|--isid=*str*	El identificador de la sesión iSCSI.
-n|--name=*str*	El nombre del destino iSCSI, por ejemplo, iqn.X.

Agregar sesiones iSCSI

Utilice vCLI para agregar una sesión iSCSI a un destino que especifique o para duplicar una sesión existente. Al duplicar las sesiones, aumenta la cantidad de sesiones predeterminada y se crean rutas de acceso adicionales a los sistemas de almacenamiento.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

- Para agregar o duplicar una sesión iSCSI, ejecute el comando siguiente:

  `esxcli iscsi session add`

  Este comando toma estas opciones:

Opción	Descripción
-A|--adapter=*str*	El nombre del adaptador de iSCSI, por ejemplo, vmhba34. Esta opción es obligatoria.
-s|--isid=*str*	El ISID de la sesión que se desea duplicar. Para encontrarlo, enumere todas las sesiones.
-n|--name=*str*	El nombre del destino iSCSI, por ejemplo, iqn.X.

Pasos siguientes

Vuelva a examinar el adaptador de iSCSI.

Quitar sesiones iSCSI

Utilice el comando vCLI para quitar una sesión iSCSI entre un adaptador de iSCSI y un destino.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

- Para quitar una sesión, ejecute el siguiente comando:

  `esxcli iscsi session remove`

  Este comando toma estas opciones:

Opción	Descripción
-A|--adapter=*str*	El nombre del adaptador de iSCSI, por ejemplo, vmhba34. Esta opción es obligatoria.
-s|--isid=*str*	El ISID de la sesión que se desea quitar. Para encontrarlo, enumere todas las sesiones.
-n|--name=*str*	El nombre del destino iSCSI, por ejemplo, iqn.X.

Pasos siguientes

Vuelva a examinar el adaptador de iSCSI.

Arrancar desde SAN iSCSI

12

Cuando se configura el host para arrancar desde una SAN, la imagen de arranque del host se almacena en uno o más LUN en el sistema de almacenamiento SAN. Cuando el host arranca, lo hace desde el LUN en la SAN, no desde su disco local.

Puede utilizar el arranque desde SAN si no desea ocuparse del mantenimiento del almacenamiento local o si tiene configuraciones de hardware sin discos, por ejemplo, sistemas blade.

ESXi admite distintos métodos de arranque desde la SAN iSCSI.

Tabla 12-1. Compatibilidad con arranque desde SAN iSCSI

iSCSI de hardware independiente	iSCSI de software
Configure el HBA de iSCSI para que arranque desde la SAN. Para obtener información sobre la configuración del HBA, consulte Configurar adaptador de iSCSI de hardware independiente para el arranque de SAN	Utilice el adaptador de iSCSI de software y un adaptador de red compatible con el formato de tabla de firmware de arranque de iSCSI (iBFT). Para obtener información, consulte *Instalar y configurar VMware ESXi*.

Este capítulo incluye los siguientes temas:

Recomendaciones generales para el arranque desde SAN iSCSI

Si planea configurar y utilizar un LUN iSCSI como dispositivo de arranque del host, siga ciertas instrucciones generales.

Las siguientes instrucciones se aplican al arranque desde iSCSI e iBFT de hardware independiente.

- Repase todas las recomendaciones del distribuidor de hardware que se utiliza en la configuración de arranque.

- Para conocer los requisitos previos y los requisitos de instalación, consulte *Instalar y configurar vSphere*.
- Utilice direcciones IP estáticas para reducir las posibilidades de conflictos con DHCP.
- Utilice LUN diferentes para particiones de arranque y almacenes de datos de VMFS.
- Configure ACL adecuadas en el sistema de almacenamiento.
  - El LUN de arranque debe ser visible solo para el host que usa el LUN. No debe permitirse que ningún otro host de la SAN vea ese LUN de arranque.
  - Si se utiliza un LUN para un almacén de datos de VMFS, varios hosts pueden compartir el LUN.
- Configure una partición de diagnóstico.
  - Solo con iSCSI de hardware independiente es posible colocar la partición de diagnóstico en el LUN de arranque. Si configura la partición de diagnóstico en el LUN de arranque, este LUN no podrá compartirse entre varios hosts. Si se utiliza un LUN independiente para la partición de diagnóstico, varios hosts pueden compartir el LUN.
  - Si el arranque se realiza desde una SAN con iBFT, no se puede configurar una partición de diagnóstico en un LUN de SAN. Para recopilar la información de diagnóstico del host, utilice vSphere ESXi Dump Collector en un servidor remoto. Para obtener información sobre ESXi Dump Collector, consulte *Instalar y configurar vCenter Server* y *Redes de vSphere*.

Preparar SAN iSCSI

Antes de configurar el host para arrancar desde un LUN iSCSI, prepare y configure la red de área de almacenamiento.

Precaución Si utiliza una instalación generada por script para instalar ESXi cuando arranca desde una SAN, debe realizar pasos especiales para evitar la pérdida de datos no intencionada.

Procedimiento

1. Conecte los cables de red, consulte cualquier guía de cableado que se aplique a la instalación.
2. Compruebe que haya conectividad IP entre el sistema de almacenamiento y el servidor.

   Compruebe la configuración de cualquier enrutador o conmutador en la red de almacenamiento. Los sistemas de almacenamiento deben poder hacer ping a los adaptadores de iSCSI en los hosts.

3 Configure el sistema de almacenamiento.

   a Cree un volumen (o LUN) en el sistema de almacenamiento desde el cual pueda arrancar el host.

   b Configure el sistema de almacenamiento para que el host tenga acceso al LUN asignado.

      Este paso podría involucrar la actualización de ACL con las direcciones IP, los nombres iSCSI y el parámetro de autenticación de CHAP que se utiliza en el host. En algunos sistemas de almacenamiento, además de proporcionar información de acceso para el host ESXi, también se debe asociar de manera explícita el LUN asignado con el host.

   c Asegúrese de que el LUN se presente correctamente al host.

   d Compruebe que ningún otro sistema tenga acceso al LUN configurado.

   e Registre el nombre iSCSI y las direcciones IP de los destinos asignados al host.

      Debe tener esta información para configurar los adaptadores de iSCSI.

Configurar adaptador de iSCSI de hardware independiente para el arranque de SAN

Si el host ESXi utiliza un adaptador de iSCSI de hardware independiente, como un HBA de QLogic, puede configurar el adaptador para que arranque desde SAN.

Este procedimiento analiza cómo habilitar el HBA de iSCSI de QLogic para arrancar desde SAN. Para obtener más información y detalles más actualizados sobre las opciones de configuración del adaptador QLogic, consulte el sitio web de QLogic.

Procedimiento

1 Inicie los soportes de instalación y reinicie el host.

2 Utilice el BIOS para establecer el host para que arranque primero desde los soportes de instalación.

3 Durante el POST del servidor, presione Ctrl+q para acceder al menú de configuración del HBA de iSCSI de QLogic.

4 Seleccione el puerto de E/S que desea configurar.

   De forma predeterminada, el modo de arranque del adaptador está deshabilitado.

5 Configure el HBA.

   a En el menú **Opciones de Fast!UTIL**, seleccione **Opciones de configuración > Configuración del adaptador de host**.

   b (opcional) Configure las siguientes opciones del adaptador de host: dirección IP del iniciador, máscara de subred, puerta de enlace, nombre iSCSI del iniciador y CHAP.

6 Configure las opciones de iSCSI.

   Consulte Configurar las opciones de arranque de iSCSI.

7 Guarde los cambios y reinicie el sistema.

Configurar las opciones de arranque de iSCSI

Configure los parámetros de arranque de iSCSI, de modo que el host ESXi pueda arrancarse desde un LUN de iSCSI.

Procedimiento

1. En el menú **Opciones de Fast!UTIL**, seleccione **Opciones de configuración > Opciones de arranque de iSCSI**.
2. Para poder establecer SendTargets, configure el modo Arranque del adaptador en **Manual**.
3. Seleccione **Configuración del dispositivo de arranque principal**.
   a. Escriba los valores de **IP de destino** y **Puerto de destino** de detección.
   b. Configure los parámetros **LUN de arranque** y **Nombre iSCSI**.
      - Si solo hay disponibles un destino de iSCSI y un LUN en la dirección de destino, deje **LUN de arranque** y **Nombre iSCSI** en blanco.

        Cuando el host alcance el sistema de almacenamiento de destino, estos cuadros de texto se rellenarán con la información correspondiente.
      - Si hay más de un destino iSCSI y un LUN disponibles, introduzca los valores para **LUN de arranque** y **Nombre iSCSI**.

   c. Guarde los cambios.
4. En el menú **Opciones de arranque de iSCSI**, seleccione el dispositivo de arranque principal.

   Al volver a examinar automáticamente el HBA, se detectarán nuevos LUN de destino.
5. Seleccione el destino iSCSI.

   Si hay más de un LUN en el destino, seleccione el identificador de LUN específico. Para ello, pulse **Entrar** después de ubicar el dispositivo iSCSI.
6. Regrese al menú **Configuración del dispositivo de arranque principal**. Después de volver a examinar, se rellenan **LUN de arranque** y **Nombre iSCSI**. Cambie el valor de **LUN de arranque** por el identificador del LUN que corresponda.

Prácticas recomendadas de almacenamiento iSCSI

13

Al utilizar ESXi con la SAN iSCSI, siga las prácticas recomendadas que ofrece VMware para evitar problemas.

Consulte a su representante de almacenamiento si su sistema de almacenamiento admite las características de aceleración de hardware de Storage API - Array Integration. Si las admite, consulte la documentación del proveedor sobre cómo habilitar la compatibilidad con la aceleración de hardware en el sistema de almacenamiento. Para obtener más información, consulte Capítulo 24 Aceleración de hardware de almacenamiento.

Este capítulo incluye los siguientes temas:

Evitar problemas en una SAN iSCSI

Al utilizar ESXi con una SAN, se deben seguir instrucciones específicas para evitar problemas en la SAN.

Tenga en cuenta las siguientes sugerencias:

- Coloque un solo almacén de datos de VMFS en cada LUN.
- No cambie la directiva de rutas de acceso que el sistema establece a menos que comprenda las consecuencias de realizar esa modificación.
- Documente todo. Incluya información sobre configuración, control de acceso, almacenamiento, conmutador, configuración de servidor y HBA iSCSI, versiones de software y firmware, y planificación del cableado de almacenamiento.
- Planificación en caso de errores:
  - Haga varias copias de los mapas de topología. Para cada elemento, tenga en cuenta lo que sucede con la SAN si el elemento presenta errores.
  - Verifique diferentes vínculos, conmutadores, HBA y otros elementos para asegurarse de no haber omitido ningún punto de error crítico en el diseño.

- Compruebe que los HBA iSCSI estén instalados en las ranuras correctas en el host ESXi, según la velocidad de bus y ranura. Equilibre la carga del bus PCI entre los buses disponibles del servidor.
- Familiarícese con los distintos puntos de supervisión en la red de almacenamiento, en todos los puntos de visibilidad, incluidos los gráficos de rendimiento de ESXi, las estadísticas del conmutador Ethernet y las estadísticas de rendimiento del almacenamiento.
- Cambie los identificadores de LUN solo cuando no haya máquinas virtuales en ejecución en los almacenes de datos de VMFS implementados en los LUN. Si cambia el identificador, las máquinas virtuales que se ejecutan en el almacén de datos de VMFS fallarán.

  Después de cambiar el identificador del LUN, debe volver a examinar el almacenamiento para restablecer el identificador en el host. Para obtener información sobre cómo volver a examinar, consulte Operaciones para volver a examinar el almacenamiento.
- Si cambia el nombre de iSCSI predeterminado del adaptador de iSCSI, asegúrese de que el nombre que introduzca sea universalmente único y que tenga el formato correcto. Para evitar problemas de acceso al almacenamiento, jamás asigne el mismo nombre iSCSI a los diferentes adaptadores, ni siquiera en hosts diferentes.

Optimización del rendimiento del almacenamiento SAN iSCSI

Hay varios factores que contribuyen a la optimización del entorno típico de SAN.

Si el entorno de red está bien configurado, los componentes de iSCSI proporcionan una capacidad de proceso adecuada y una latencia suficientemente baja para iniciadores y destinos iSCSI. Si la red está congestionada y los vínculos, conmutadores y enrutadores están saturados, el rendimiento de iSCSI se verá afectado y es posible que no sea el adecuado para los entornos de ESXi.

Rendimiento del sistema de almacenamiento

El rendimiento del sistema de almacenamiento es uno de los principales factores que contribuye al rendimiento de todo el entorno de iSCSI.

Si se producen problemas con el rendimiento del sistema de almacenamiento, consulte la documentación del proveedor del sistema de almacenamiento para acceder a toda la información relevante.

Al asignar LUN, recuerde que puede acceder a todos los LUN compartidos a través de una serie de hosts, y que pueden ejecutarse varias máquinas virtuales en cada host. Un LUN utilizado por el host ESXi puede atender operaciones de E/S desde varias aplicaciones diferentes que se ejecuten en distintos sistemas operativos. Debido a esta carga de trabajo diversa, el grupo RAID que contiene los LUN de ESXi no debe incluir LUN que utilicen otros hosts y que no ejecuten ESXi para aplicaciones de uso intensivo de E/S.

Habilite el almacenamiento en caché de lectura y de escritura.

El equilibrio de carga es el proceso de distribuir solicitudes de E/S de servidores en todos los SP disponibles y las rutas de acceso a servidores de hosts asociadas. El objetivo es optimizar el rendimiento en términos de capacidad de proceso (E/S por segundo, megabytes por segundo o tiempos de respuesta).

Los sistemas de almacenamiento SAN requieren un rediseño y ajuste continuos para garantizar que las operaciones de E/S sean equilibradas en todas las rutas de acceso del sistema de almacenamiento. Para cumplir con este requisito, distribuya las rutas de acceso a los LUN entre todos los SP. De esa manera, se podrá proporcionar un equilibrio de carga óptimo. Una supervisión exhaustiva indica en qué momento es necesario volver a equilibrar manualmente la distribución de LUN.

Para ajustar sistemas de almacenamiento equilibrados estadísticamente se deben supervisar estadísticas de rendimiento específicas (como operaciones de E/S por segundo, bloques por segundo y tiempos de respuesta), y es necesario distribuir la carga de trabajo de LUN para propagar la carga de trabajo en todos los SP.

Rendimiento del servidor con iSCSI

Para garantizar un rendimiento óptimo del host ESXi, debe tener en cuenta varios factores.

Cada aplicación del servidor debe tener acceso a su almacenamiento designado con las condiciones siguientes:

- Velocidad de E/S alta (cantidad de operaciones de E/S por segundo)
- Alta capacidad de proceso (megabytes por segundo)
- Latencia mínima (tiempos de respuesta)

Dado que cada aplicación tiene distintos requisitos, puede cumplir estos objetivos eligiendo un grupo RAID adecuado en el sistema de almacenamiento.

Para alcanzar los objetivos de rendimiento, siga estas directrices:

- Coloque cada LUN en un grupo RAID que proporcione los niveles de rendimiento necesarios. Supervise las actividades y el uso de recursos de otros LUN en el grupo RAID asignado. Es posible que un grupo RAID de alto rendimiento que tiene demasiadas aplicaciones que realizan operaciones de E/S en él no cumpla con los objetivos de rendimiento requeridos por una aplicación que se ejecuta en el host ESXi.
- Para lograr la máxima capacidad de proceso de todas las aplicaciones en el host durante el período máximo, instale suficientes adaptadores de red o adaptadores de hardware de iSCSI. La propagación de E/S en varios puertos proporciona una capacidad de proceso más rápida y menos latencia para cada aplicación.
- Para proporcionar redundancia para iSCSI de software, asegúrese de que el iniciador esté conectado a todos los adaptadores de red usados para la conectividad de iSCSI.

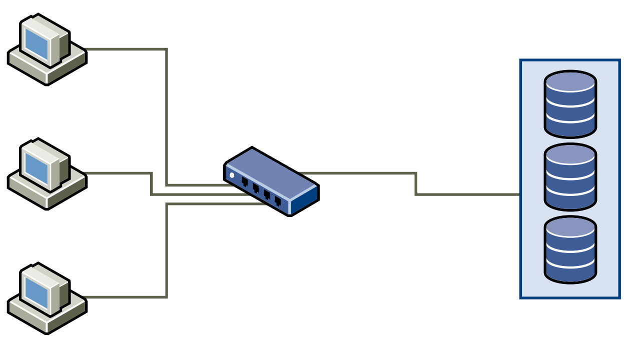
- Cuando se asignan LUN o grupos RAID a sistemas ESXi, recuerde que varios sistemas operativos usan y comparten ese recurso. El rendimiento de LUN requerido por el host ESXi podría ser mucho mayor que cuando se usan máquinas físicas normales. Por ejemplo, si espera ejecutar cuatro aplicaciones de uso intensivo de E/S, asigne el cuádruple de capacidad de rendimiento al LUN de ESXi.
- Cuando se usan varios sistemas ESXi con vCenter Server, aumentan los requisitos de rendimiento de almacenamiento.
- La cantidad de E/S pendientes requerida por las aplicaciones que se ejecutan en un sistema ESXi debe coincidir con la cantidad de E/S que puede manejar la SAN.

Rendimiento de la red

Una SAN típica consiste en una recopilación de equipos conectados a una recopilación de sistemas de almacenamiento a través de una red de conmutadores. Varios equipos acceden generalmente al mismo almacenamiento.

La siguiente imagen muestra varios sistemas informáticos conectados a un sistema de almacenamiento a través de un solo conmutador Ethernet. En esta configuración, cada sistema está conectado a través de un solo vínculo Ethernet al conmutador. El conmutador está conectado al sistema de almacenamiento a través de un solo vínculo Ethernet.

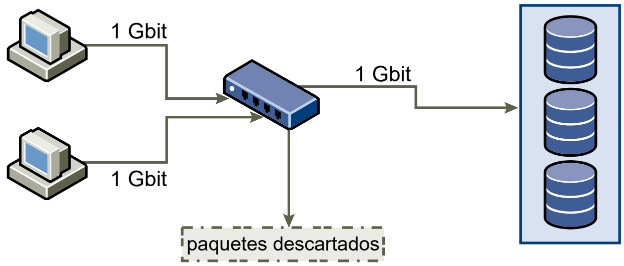
Figura 13-1. Conectar un solo vínculo Ethernet con el almacenamiento



Cuando los sistemas leen datos del almacenamiento, el almacenamiento responde enviando datos suficientes para completar el vínculo entre los sistemas de almacenamiento y el conmutador Ethernet. Es poco probable que un sistema o una máquina virtual usen el total de la velocidad de red. Sin embargo, esta situación puede darse cuando muchos sistemas comparten el mismo dispositivo de almacenamiento.

Cuando se escriben datos en el almacenamiento, varios sistemas o máquinas virtuales pueden intentar completar los vínculos. Como resultado, es posible que el conmutador que une los sistemas y el sistema de almacenamiento descarte paquetes de red. El descarte de datos podría ocurrir debido a que el conmutador tiene más tráfico para enviar al sistema de almacenamiento del que puede transmitir un solo vínculo. La cantidad de datos que puede transmitir el conmutador está limitada por la velocidad del vínculo entre este y el sistema de almacenamiento.

Figura 13-2. Paquetes descartados



La recuperación de datos de los paquetes de red descartados provoca una gran degradación del rendimiento. Además del tiempo dedicado a determinar que se descartaron datos, la retransmisión utiliza ancho de banda que, de lo contrario, podría usarse para transacciones actuales.

El protocolo Transmission Control Protocol (TCP) traslada el tráfico iSCSI en la red. TCP es un protocolo de transmisión confiable que garantiza que se vuelva a intentar la transmisión de los paquetes descartados para que estos alcancen, eventualmente, su destino. TCP está diseñado para recuperar datos a partir de paquetes descartados y volver a transmitirlos de forma rápida y sencilla. Sin embargo, cuando el conmutador descarta paquetes con cualquier regularidad, el rendimiento de red se ve afectado. La red se congestiona con las solicitudes para volver a enviar datos y con los paquetes reenviados. Se transfieren menos datos que en una red sin congestión.

La mayoría de los conmutadores Ethernet pueden guardar datos en búfer, es decir, almacenarlos. Esta técnica da la misma oportunidad de llegar al destino a todos los dispositivos que intentan enviar datos. La capacidad para almacenar en búfer algunas transmisiones, combinada con muchos sistemas que limitan el número de comandos pendientes, reduce las transmisiones a ráfagas pequeñas. Las ráfagas de varios sistemas se pueden enviar a su vez a un sistema de almacenamiento.

Si las transacciones son grandes y hay varios servidores que envían datos a través de un puerto de conmutador único, se puede superar la capacidad de almacenamiento en búfer. En este caso, el conmutador descarta los datos que no puede enviar y el sistema de almacenamiento debe solicitar la retransmisión del paquete descartado. Por ejemplo, si un conmutador Ethernet puede almacenar en búfer 32 KB, pero el servidor envía 256 KB al dispositivo de almacenamiento, algunos de los datos se descartarán.

La mayoría de los conmutadores administrados proporcionan información sobre paquetes descartados, algo similar a lo siguiente:

```
*: interface is up
IHQ: pkts in input hold queue      IQD: pkts dropped from input queue
OHQ: pkts in output hold queue     OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec)           RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec)           TXPS: tx rate (pkts/sec)
TRTL: throttle count
```

Tabla 13-1. Información de conmutador de muestra

Interfaz	IHQ	IQD	OHQ	OQD	RXBS	RXPS	TXBS	TXPS	TRTL
* GigabitEthernet0/1	3	9922	0	0	476303000	62273	477840000	63677	0

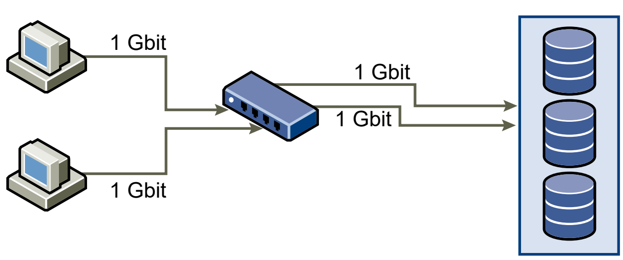
En este ejemplo de un conmutador Cisco, el ancho de banda usado es de 476.303.000 bits/segundo, que es menos de la mitad de la velocidad de cable. El puerto almacena en búfer los paquetes entrantes, pero descarta varios paquetes. La línea final de este resumen de interfaz indica que este puerto ya descartó casi 10.000 paquetes entrantes en la columna IQD.

Los cambios de configuración para evitar este problema incluyen comprobar que los diversos vínculos Ethernet de entrada no estén canalizados a un vínculo de salida, ya que provocaría un vínculo con exceso de suscripciones. Cuando varios vínculos que transmiten casi al límite de capacidad se cambian por una menor cantidad de vínculos, es posible que se produzca un exceso de suscripciones.

Por lo general, las aplicaciones o los sistemas que escriben muchos datos en el almacenamiento deben evitar compartir vínculos Ethernet con un dispositivo de almacenamiento. Estos tipos de aplicaciones tienen mejor rendimiento con varias conexiones a los dispositivos de almacenamiento.

La imagen Varias conexiones del conmutador al almacenamiento muestra varias conexiones del conmutador al almacenamiento.

Figura 13-3. Varias conexiones del conmutador al almacenamiento



La utilización de VLAN o VPN no proporciona una solución adecuada al problema de exceso de suscripciones de vínculos en configuraciones compartidas. Las VLAN y otras particiones virtuales de una red proporcionan una forma de designar una red lógicamente. Sin embargo, no cambian las capacidades físicas de los vínculos y los troncos entre conmutadores. Cuando el tráfico de almacenamiento y otros tipos de tráfico de red comparten conexiones físicas, es posible que se produzcan suscripciones excesivas y pérdida de paquetes. Lo mismo ocurre con las VLAN que comparten troncos entre conmutadores. El diseño de rendimiento de una SAN debe tener en cuenta las limitaciones físicas de la red, no las asignaciones lógicas.

Comprobar estadísticas del conmutador Ethernet

Muchos conmutadores Ethernet ofrecen diferentes métodos para supervisar el estado del conmutador.

Los conmutadores que tienen puertos funcionando cerca de su capacidad de proceso máxima la mayor parte del tiempo no brindan un rendimiento óptimo. Si tiene puertos en una SAN iSCSI funcionando cerca del máximo, reduzca la carga. Si el puerto está conectado con un sistema ESXi o almacenamiento iSCSI, puede reducir la carga a través del equilibrio de carga manual.

Si el puerto está conectado entre varios conmutadores o enrutadores, considere instalar vínculos adicionales entre estos componentes para soportar mayor carga. Generalmente, los conmutadores Ethernet también ofrecen información sobre errores de transmisión, paquetes en cola y paquetes Ethernet descartados. Si el conmutador informa regularmente cualquiera de estas condiciones en puertos que se usen para el tráfico iSCSI, el rendimiento de la SAN iSCSI no será bueno.

Administrar dispositivos de almacenamiento

14

Administre los dispositivos de almacenamiento locales y en red a los que tiene acceso el host ESXi.

Este capítulo incluye los siguientes temas:

Características de los dispositivos de almacenamiento

Cuando el host ESXi se conecta a los sistemas de almacenamiento basado en bloques, los dispositivos de almacenamiento o LUN que admiten ESXi se vuelven disponibles para el host.

Después de registrar los dispositivos en el host, puede mostrar todos los dispositivos en red y locales que hay disponibles y revisar su información. Si se usan complementos de múltiples rutas de terceros, los dispositivos de almacenamiento disponibles por medio de los complementos también aparecen en la lista.

Nota Si una matriz admite el acceso a unidades lógicas asimétricas (Asymmetric Logical Unit Access, ALUA) implícitas y solo tiene rutas de acceso en espera, se produce un error en el registro del dispositivo. El dispositivo se puede registrar con el host después de que la instancia de destino activa una ruta de acceso en espera y el host la detecta como activa. El parámetro `/Disk/FailDiskRegistration` avanzado del sistema controla este comportamiento del host.

Se puede ver una lista independiente de los dispositivos de almacenamiento disponibles para un adaptador en particular.

Generalmente, al consultar los dispositivos de almacenamiento, se ve la siguiente información.

Tabla 14-1. Información de dispositivos de almacenamiento

Información de dispositivos de almacenamiento	Descripción
Nombre	También llamado Nombre para mostrar. Es un nombre que el host ESXi asigna al dispositivo según el tipo de almacenamiento y el fabricante. En general, puede cambiar este nombre por uno de su elección. Consulte Cambiar nombre de los dispositivos de almacenamiento.
Identificador	Un identificador universalmente único que es intrínseco al dispositivo. Consulte Identificadores y nombres de dispositivos de almacenamiento.
Estado operativo	Indica si el dispositivo está conectado o desconectado. Consulte Separar dispositivos de almacenamiento.
LUN	Número de unidad lógica (LUN) en el destino SCSI. El número LUN se obtiene del sistema de almacenamiento. Si un destino tiene un solo LUN, el número LUN siempre es cero (0).
Tipo	Tipo de dispositivo, por ejemplo, disco o CD-ROM.
Tipo de unidad	Información que especifica si el dispositivo es una unidad flash o una unidad HDD regular. Para obtener más información sobre las unidades flash y los dispositivos NVMe, consulte Capítulo 15 Trabajar con dispositivos flash.
Transporte	Protocolo de transporte que usa el host para acceder al dispositivo. El protocolo depende del tipo de almacenamiento que se usa. Consulte Tipos de almacenamiento físico.
Capacidad	Capacidad total del dispositivo de almacenamiento.
Propietario	El complemento, como NMP o el complemento de un tercero, que el host usa para administrar las rutas de acceso al dispositivo de almacenamiento. Consulte Administración de la ruta de acceso y arquitectura de almacenamiento acoplable.
Aceleración de hardware	Información sobre si el dispositivo de almacenamiento asiste al host en las operaciones de administración de máquinas virtuales. El estado puede ser Compatible, No compatible o Desconocido. Consulte Capítulo 24 Aceleración de hardware de almacenamiento.
Formato de sector	Indica si el dispositivo usa un formato tradicional, 512n o de sector avanzado, como 512e o 4Kn. Consulte Formatos de sector de dispositivos.
Ubicación	Una ruta de acceso al dispositivo de almacenamiento en el directorio `/vmfs/devices/`.
Formato de partición	Un esquema de particiones que usa el dispositivo de almacenamiento. Puede ser un formato de registro de arranque maestro (Master Boot Record, MBR) o de tabla de particiones GUID (GUID partition table, GPT). Los dispositivos GPT pueden admitir almacenes de datos mayores a 2 TB. Consulte Formatos de sector de dispositivos.
Particiones	Particiones principales y lógicas, incluido un almacén de datos de VMFS, si está configurado.
Directivas de múltiples rutas	Directiva de selección de rutas de acceso y directiva de tipo de matriz de almacenamiento que usa el host para administrar las rutas de acceso al almacenamiento. Consulte Capítulo 18 Descripción de múltiples rutas y conmutación por error.
Rutas de acceso	Rutas de acceso que se utilizan para acceder al almacenamiento y a su estado. Consulte Deshabilitar rutas de acceso de almacenamiento.

Mostrar dispositivos de almacenamiento de un host ESXi

Muestre todos los dispositivos de almacenamiento disponibles para un host ESXi. Si se utiliza algún complemento de múltiples rutas de terceros, los dispositivos de almacenamiento disponibles por medio de los complementos también aparecen en la lista.

La vista Dispositivos de almacenamiento permite enumerar los dispositivos de almacenamiento de los hosts, analizar la información y modificar las propiedades.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Dispositivos de almacenamiento**.

   Todos los dispositivos de almacenamiento disponibles para el host se enumeran en la tabla Dispositivos de almacenamiento.

4 Para ver los detalles de un dispositivo específico, seleccione el dispositivo en la lista.

5 Utilice los iconos para realizar tareas de administración de almacenamiento básicas.

   La disponibilidad de ciertos iconos depende del tipo de dispositivo y de la configuración.

Icono	Descripción
Actualizar	Actualice la información sobre los adaptadores de almacenamiento, la topología y los sistemas de archivos.
Separar	Separe el dispositivo seleccionado del host.
Asociar	Asocie el dispositivo seleccionado al host.
Cambiar nombre	Cambie el nombre para mostrar del dispositivo seleccionado.
Encender LED	Encienda el LED del localizador de los dispositivos seleccionados.
Apagar LED	Apague el LED del localizador de los dispositivos seleccionados.
Marcar como discos flash	Marque los dispositivos seleccionados como discos flash.
Marcar como disco HDD	Marque los dispositivos seleccionados como discos HDD.
Marcar como local	Marque los dispositivos seleccionados como locales para el host.
Marcar como remoto	Marque los dispositivos seleccionados como remotos para el host.
Borrar particiones	Borre las particiones de los dispositivos seleccionados.
Marcar como reservado de forma perenne	Marque el dispositivo seleccionado como reservado de forma perenne.
Desmarcar como reservado de forma perenne	Borre la reserva perenne del dispositivo seleccionado.

6 Use las siguientes pestañas para acceder a información adicional y modificar las propiedades del dispositivo seleccionado.

Tabulador	Descripción
Propiedades	Vea las propiedades y características del dispositivo. Vea y modifique las directivas de múltiples rutas para el dispositivo.
Rutas de acceso	Muestre las rutas de acceso disponibles para el dispositivo. Permite deshabilitar o habilitar una ruta de acceso seleccionada.
Detalles de particiones	Muestra información sobre las particiones y sus formatos.

Mostrar dispositivos de almacenamiento para un adaptador

Muestre una lista de dispositivos de almacenamiento a los que se pueda acceder a través de un adaptador de almacenamiento específico en el host ESXi.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento**.

   Todos los adaptadores de almacenamiento instalados en el host se enumeran en la tabla Adaptadores de almacenamiento.

4 Seleccione el adaptador en la lista y haga clic en la pestaña **Dispositivos**.

   Aparecen los dispositivos de almacenamiento a los que puede acceder el host a través del adaptador.

5 Utilice los iconos para realizar tareas de administración de almacenamiento básicas.

   La disponibilidad de ciertos iconos depende del tipo de dispositivo y de la configuración.

Icono	Descripción
Actualizar	Actualice la información sobre los adaptadores de almacenamiento, la topología y los sistemas de archivos.
Separar	Separe el dispositivo seleccionado del host.
Asociar	Asocie el dispositivo seleccionado al host.
Cambiar nombre	Cambie el nombre para mostrar del dispositivo seleccionado.

Formatos de sector de dispositivos

ESXi admite dispositivos de almacenamiento con formatos de sector tradicionales y avanzados. Cuando se habla de almacenamiento, un sector es una subdivisión de una pista en un disco o dispositivo de almacenamiento. Cada sector almacena una cantidad fija de datos.

En esta tabla, se presentan los formatos de dispositivos de almacenamiento diferentes que ESXi admite.

Formato de dispositivo de almacenamiento	Emulación de software de ESXi	Tamaño del sector lógico	Tamaño del sector físico	Almacén de datos de VMFS
512n	N/C	512	512	VMFS5 y VMFS6 (predeterminado)
512e	N/C	512	4.096	VMFS5 y VMFS56 (predeterminado) **Nota** Los dispositivos de almacenamiento 512e locales no admiten VMFS5.
4Kn	512	4.096	4.096	VMFS 6

Formato nativo de 512 bytes

ESXi es compatible con los dispositivos de almacenamiento 512n tradicionales que utilizan un tamaño de sector nativo de 512 bytes.

Formato de emulación de 512 bytes

Debido a la creciente demanda de mayor capacidad, la industria del almacenamiento incorporó formatos avanzados, como la emulación de 512 bytes, o 512e. 512e es el formato avanzado en el cual el tamaño del sector físico es de 4.096 bytes, pero el sector lógico emula el tamaño del sector de 512 bytes. Los dispositivos de almacenamiento que usan el formato 512e pueden admitir aplicaciones y sistemas operativos invitados heredados. Estos dispositivos funcionan como un paso intermedio a las unidades de sector 4Kn.

Formato nativo de 4K con emulación de software

Otro formato avanzado que ESXi admite es la tecnología de sector 4Kn. En los dispositivos 4Kn, los sectores lógicos y físicos son de 4.096 bytes (4 KiB) de longitud. El dispositivo no tiene una capa de emulación, pero expone su tamaño de sector físico 4Kn directamente a ESXi.

ESXi detecta y registra los dispositivos 4Kn y los emula automáticamente como 512e. El dispositivo se presenta a las capas superiores en ESXi como 512e. Pero los sistemas operativos invitados siempre lo ven como un dispositivo 512n. Puede seguir utilizando las máquinas virtuales existentes con aplicaciones y sistemas operativos invitados heredados en el host con los dispositivos 4Kn.

Al utilizar dispositivos 4Kn, se deben tener en cuenta las siguientes consideraciones:

- ESXi solo admite discos HDD SAS y SATA 4Kn locales.
- ESXi no admite dispositivos NVMe y SSD 4Kn o dispositivos 4Kn como RDM.
- ESXi solo puede arrancar desde un dispositivo 4Kn con UEFI.
- Puede utilizar el dispositivo 4Kn para configurar una partición de volcado de núcleo y un archivo de volcado de núcleo.

- Solo el complemento NMP puede reclamar los dispositivos 4Kn. No se puede usar HPP para la notificación de estos dispositivos.
- Con vSAN, puede utilizar solo HDD con capacidad 4Kn para las matrices híbridas de vSAN. Para obtener información, consulte el documento *Administrar VMware vSAN*.
- Debido a la capa de emulación de software, el rendimiento de los dispositivos 4Kn depende de la alineación de las operaciones de E/S. Para obtener el mejor rendimiento, ejecute cargas de trabajo que emitan principalmente operaciones de E/S alineadas con 4K.
- Las cargas de trabajo que acceden al dispositivo 4Kn emulado directamente mediante E/S de dispersión o recopilación (Scatter-Gather I/O, SGIO) deben emitir operaciones de E/S compatibles con el disco 512e.

Ejemplo: Determinar el formato de dispositivo

Para determinar si el dispositivo utiliza el formato 512n, 512e o 4Kn, ejecute el siguiente comando.

```
esxcli storage core device capacity list
```

Los resultados de ejemplo siguientes muestran el tipo de formato.

```
Device                Physical Blocksize  Logical Blocksize  Logical Block Count
Size  Format Type
--------------------  ------------------  -----------------  -------------------
-----------  -----------
naa.5000xxxxxxxxx36f                 512                512           2344225968  1144641
MiB  512n
naa.5000xxxxxxxxx030                4096                512           3516328368  1716957
MiB  4Kn SWE
naa.5000xxxxxxxxx8df                 512                512           2344225968  1144641
MiB  512n
naa.5000xxxxxxxxx4f4                4096                512           3516328368  1716957
MiB  4Kn SWE
```

Identificadores y nombres de dispositivos de almacenamiento

En el entorno de ESXi, cada dispositivo de almacenamiento se identifica con varios nombres.

Identificadores de dispositivo

Según el tipo de almacenamiento, el host ESXi utiliza distintos algoritmos y convenciones para generar un identificador para cada dispositivo de almacenamiento.

Identificadores provistos por el almacenamiento

El host ESXi consulta a un dispositivo de almacenamiento de destino el nombre del dispositivo. A partir de los metadatos devueltos, el host extrae o genera un identificador único

para el dispositivo. El identificador se basa en estándares de almacenamiento específico, es persistente y único en todos los hosts; además, tiene uno de los formatos siguientes:

- naa.*xxx*
- eui.*xxx*
- t10.*xxx*

Identificador basado en rutas

Cuando el dispositivo no proporciona un identificador, el host genera un nombre mpx.*path*, donde *path* representa la primera ruta de acceso al dispositivo, por ejemplo, `mpx.vmhba1:C0:T1:L3`. Este identificador puede usarse de la misma forma que el identificador proporcionado por el almacenamiento.

El identificador mpx.*ruta* se crea para dispositivos locales asumiendo que los nombres de ruta son únicos. Sin embargo, este identificador no es único ni persistente y puede cambiar después de reiniciar todos los sistemas.

Generalmente, la ruta de acceso al dispositivo tiene el formato siguiente:

vmhba*Adapter*:C*Channel*:T*Target*:L*LUN*

- vmhba*Adapter* es el nombre del adaptador de almacenamiento. El nombre se refiere al adaptador físico en el host, no a la controladora SCSI que usan las máquinas virtuales.
- C*Channel* es el número de canal de almacenamiento.

  Los adaptadores de iSCSI de software y los adaptadores de hardware dependiente utilizan el número de canal para mostrar varias rutas de acceso al mismo destino.
- T*Target* es el número de destino. El host determina la numeración de destinos y esta puede cambiar cuando las asignaciones de destinos visibles para el host cambian. Los destinos compartidos entre distintos hosts no pueden tener el mismo número de destino.
- L*LUN* es el número LUN que muestra la posición del LUN en el destino. El número LUN se obtiene del sistema de almacenamiento. Si un destino tiene un solo LUN, el número LUN siempre es cero (0).

Por ejemplo, `vmhba1:C0:T3:L1` representa al LUN1 en el destino 3 al que se accede a través del adaptador de almacenamiento vmhba1 y del canal 0.

Identificador heredado

Además del identificador proporcionado por el dispositivo o mpx.*ruta*, ESXi genera un nombre heredado alternativo para cada dispositivo. El identificador tiene el formato siguiente:

vml.*number*

El identificador heredado incluye una serie de dígitos que son únicos para el dispositivo. El identificador puede proceder en parte de los metadatos que se obtienen a través del comando SCSI INQUIRY. En los dispositivos no locales que no proporcionan identificadores SCSI INQUIRY, el identificador vml.*number* se utiliza como el único identificador exclusivo disponible.

Ejemplo: Mostrar nombres de dispositivo en vSphere CLI

Puede utilizar el comando `esxcli storage core device list` para mostrar todos los nombres de dispositivo en la CLI de vSphere. El resultado es similar al ejemplo siguiente:

```
# esxcli storage core device list
naa.XXX
      Display Name: DGC Fibre Channel Disk(naa.XXX)
      ...
      Other UIDs: vml.000XXX
mpx.vmhba1:C0:T0:L0
   Display Name: Local VMware Disk (mpx.vmhba1:C0:T0:L0)
   ...
   Other UIDs: vml.0000000000XYZ
```

Dispositivos NVMe con identificadores de dispositivo NGUID

Para los dispositivos NVMe, ESXi genera identificadores de dispositivos en función de la información que recupera de los dispositivos. Por lo general, los dispositivos NVMe admiten identificadores con los formatos EUI64 o NGUID, o bien utilizan ambos formatos. NGUID es un identificador global único de espacio de nombres que utiliza el formato de designador de 16 bits EUI64.

Para los dispositivos que solo admiten el formato NGUID, los cambios de identificador de dispositivo generados por el host dependen de la versión de ESXi. El host ESXi con las versiones 6.7 y anteriores creó el identificador t10.*xxx_número_de_serie_de_controladora*. A partir de la versión 6.7 Update 1, el host crea dos identificadores: eui.*xxx (NGUID)* como el principal, y t10.*xxx_número_de_serie_de_controladora* como el principal alternativo.

Formatos de identificador que admite el dispositivo		Identificador de dispositivo generado por el host	
Formato de identificador EUI64	**Formato de identificador NGUID**	**ESXi 6.7 y versiones anteriores**	**ESXi 6.7 Update 1 y posterior**
yes	yes	t10.*xxx_ EUI64*	t10.*xxx_ EUI64*
yes	no	t10.*xxx_ EUI64*	t10.*xxx_ EUI64*
no	yes	t10.*xxx_ número_ de_ serie _ de_ controladora*	eui.*xxx (NGUID)* como identificador principal t10.*xxx_ número_ de_ serie _ de_ controladora* como identificador principal alternativo

Nota Si el host tiene dispositivos que solo tienen el formato NGUID y actualiza el host a ESXi 7.0.x desde una versión anterior, el identificador del dispositivo cambia de t10.*xxx_ número_ de_ serie_ de_ controladora* a eui.*xxx (NGUID)* en todo el entorno de ESXi. Si utiliza el identificador del dispositivo en cualquiera de los scripts de cliente, debe reflejar este cambio de formato.

Verificar la asignación entre identificadores de dispositivo principales y alternativos

Utilice el comando `esxcli storage core device uidmap list` para comprobar los identificadores de dispositivo. El resultado es similar al siguiente:

```
 esxcli storage core device uidmap list
eui.0000xyz.....
   Primary UID: eui.0000xyz.....
   Alternative Primary UIDs: t10.0000abc....
   Legacy UID: vml.0000000000766d68....
   Alternative Legacy UIDs: vml.000000000080906....
```

Actualizar hosts ESXi sin estado con dispositivos NVMe solo de NGUID a la versión 7.0.x

Si el entorno contiene hosts de ESXi sin estado de las versiones 6.7 y anteriores, e incluye dispositivos NVMe que solo admiten el formato NGUID, se usará el flujo de trabajo actual para actualizar los hosts a la versión 7.0.x.

Cuando actualice los hosts sin estado de las versiones 6.7 y anteriores a la versión 7.0.x, siga los pasos que aparecen a continuación para conservar la configuración de almacenamiento. Si se realiza la actualización sin seguir las instrucciones, puede que no toda la configuración de almacenamiento capturada en los perfiles de host se conserve a lo largo de la actualización. Como resultado, podrían producirse errores de cumplimiento de perfil de host después de la actualización.

Requisitos previos

- El entorno contiene hosts ESXi sin estado de las versiones 6.7 o anteriores.
- El entorno incluye dispositivos NVMe que solo admiten el formato NGUID.

Procedimiento

1 Determine si el host contiene dispositivos NVMe que solo tienen el formato NGUID.

   a Compruebe que el proveedor del dispositivo es NVMe.

   Utilice el siguiente comando como ejemplo.

```
# esxcli storage core device list -d eui.f04xxxxxxxxx0000000100000001
eui.f04xxxxxxxxx0000000100000001
Display Name: Local NVMe Disk (eui.f04xxxxxxxxx0000000100000001)
Has Settable Display Name: true
Devfs Path: /vmfs/devices/disks/eui.f04bxxxxxxxxx0000000100000001
Vendor: NVMe
```

   La línea `Vendor: NVMe` indica que el dispositivo es NVMe.

   b Determine qué HBA está conectado al dispositivo NVMe.

```
# esxcli storage core adapter device list
HBA    Device UID
------ ------------------------------
vmhba2 eui.f04xxxxxxxxx0000000100000001
```

   c Obtenga la información de espacio de nombres para el dispositivo NVMe mediante el HBA y el identificador del espacio de nombres.

```
# esxcli nvme device namespace get -A vmhba2 -n 1
Namespace Identify Info:
Namespace Size: 0xe8e088b0 Logical Blocks
Namespace Capacity: 0xe8e088b0 Logical Blocks
. . .
NVM Capacity: 0x1d1c1116000
Namespace Globally Unique Identifier: 0xf04xxxxxxxxx0000000100000001
IEEE Extended Unique Identifier: 0x0
```

   En el resultado, para un dispositivo NVMe que solo tenga el formato NGUID, el campo `IEEE Extended Unique Identifier` contiene 0 y `Namespace Globally Unique Identifier` contiene un valor distinto de cero.

2 Para conservar la configuración de almacenamiento capturada en el perfil de host, siga los pasos que aparecen a continuación cuando actualice un host sin estado a la versión 7.0.x.

   a Antes de la actualización, almacene `esx.conf` en una ubicación persistente.

     Por ejemplo, puede copiar el archivo `esx.conf` en un almacén de datos de VMFS.

     ```
     # cp /etc/vmware/esx.conf /vmfs/volumes/datastore1/
     ```

   b Actualice el host.

     Tras la actualización, el host no es compatible con el perfil y puede que permanezca en modo de mantenimiento.

   c Aplique la configuración del dispositivo para dispositivos NVMe que solo tengan el formato NGUID mediante formatos de identificador nuevos.

     Ejecute el siguiente comando desde el host e indique la ubicación del archivo `esx.conf`.

     ```
      # python ./usr/lib/vmware/nvme-nguid-support/bin/nguidApplySettings.pyc -l /vmfs/
     volumes/datastore1/
     ```

3 Copie la configuración del host y restablezca las personalizaciones de host.

   a En vSphere Client, haga clic en **Inicio > Directivas y perfiles > Perfiles de host** y haga clic en el perfil asociado al host.

   b Haga clic en la pestaña **Configurar > Copiar configuración del host** y seleccione el host.

   c Para restablecer las personalizaciones, desplácese hasta el host y seleccione **Perfiles de host > Restablecer personalizaciones de host** del menú contextual.

4 En el menú contextual del host, seleccione **Perfiles de host > Corregir**.

  El host pasa a ser compatible.

5 Reinicie el host y salga del modo de mantenimiento.

Ejemplo: Actualizar el host ESXi sin conservar la configuración de almacenamiento

Si no conserva la configuración de almacenamiento capturada en el perfil de host, se pueden producir algunos errores de conformidad en el host tras actualizarlo. En este caso, copie la configuración del host y restablezca las personalizaciones de host.

Cambiar nombre de los dispositivos de almacenamiento

El host ESXi asigna un nombre para mostrar a los dispositivos de almacenamiento según el tipo de almacenamiento y el fabricante. Se puede cambiar el nombre para mostrar del dispositivo.

No se puede cambiar el nombre de ciertos tipos de dispositivos locales.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Dispositivos de almacenamiento**.

4 Seleccione el dispositivo al que desea cambiar el nombre y haga clic en **Cambiar nombre**.

5 Cambie el nombre del dispositivo a un nombre descriptivo.

Operaciones para volver a examinar el almacenamiento

Cuando realiza tareas de administración de almacenamiento o hace cambios en la configuración de SAN, es posible que necesite volver a examinar el almacenamiento.

Cuando realiza operaciones de administración del almacén de datos de VMFS, como crear un almacén de datos de VMFS o RDM, agregar una extensión y aumentar o eliminar un almacén de datos de VMFS, el host o vCenter Server vuelven a examinar el almacenamiento y lo actualizan automáticamente. Puede deshabilitar la característica automática para volver a examinar si desactiva la opción Filtro para volver a examinar el host. Consulte Desactivar los filtros de almacenamiento.

En ciertos casos, debe volver a examinar de forma manual. Puede volver a examinar todo el almacenamiento disponible para el host o para todos los host de una carpeta, un clúster o un centro de datos.

Si los cambios que realiza son exclusivos para el almacenamiento conectado a través de un adaptador específico, vuelva a examinar ese adaptador.

Vuelva a examinar de forma manual cada vez que haga uno de los cambios siguientes:

- Al dividir en zonas una matriz de discos nueva en una SAN.
- Al crear LUN nuevos en una SAN.
- Al cambiar el enmascaramiento de las rutas de acceso en un host.
- Reconectar un cable.
- Al cambiar la configuración de CHAP (solo iSCSI).
- Al agregar o quitar direcciones estáticas o de detección (solo iSCSI).
- Al agregar un solo host a vCenter Server después de editar o quitar de vCenter Server un almacén de datos compartido por los hosts de vCenter Server y el mismo host.

Importante Si vuelve a examinar cuando una ruta de acceso no está disponible, el host quita la ruta de acceso de la lista de rutas de acceso al dispositivo. La ruta de acceso vuelve a aparecer en la lista cuando vuelve a estar disponible y vuelve a funcionar.

Realizar la operación para volver a examinar el almacenamiento

Cuando se realizan cambios en la configuración de SAN, es posible que haya que volver a examinar el almacenamiento. Puede volver a examinar todo el almacenamiento disponible para

el host ESXi, el clúster o el centro de datos. Si los cambios que realiza son aislados para un almacenamiento al que se accede a través de un host específico, vuelva a examinar solo este host.

Procedimiento

1 En el navegador de objetos de vSphere Client, desplácese hasta un host, un clúster, un centro de datos o una carpeta que contenga hosts.

2 En el menú contextual, seleccione **Almacenamiento > Volver a examinar almacenamiento**.

3 Especifique la extensión del nuevo análisis.

Opción	Descripción
Buscar nuevos dispositivos de almacenamiento	Vuelva a examinar todos los adaptadores para detectar nuevos dispositivos de almacenamiento. Si se detectan nuevos dispositivos, estos aparecen en la lista de dispositivos.
Buscar nuevos volúmenes VMFS	Vuelva a examinar todos los dispositivos de almacenamiento para detectar almacenes de datos nuevos que se hayan agregado desde la última exploración. Todos los almacenes de datos nuevos aparecen en la lista de almacenes de datos.

Realizar la operación para volver a examinar el adaptador

Cuando se hacen cambios en la configuración de SAN y los cambios son exclusivos para el almacenamiento al que se accede a través de un adaptador específico en un host ESXi, vuelva a examinar solo ese adaptador.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione en la lista el adaptador que desea volver a examinar.

4 Haga clic en el icono **Volver a examinar adaptador**.

Cambiar la cantidad de dispositivos de almacenamiento examinados

El rango de identificadores de LUN examinados para un host ESXi se encuentra entre 0 y 16.383. ESXi ignora los identificadores de LUN superiores a 16.383. El parámetro `Disk.MaxLUN` configurable controla el rango de identificadores de LUN examinados. El parámetro tiene un valor predeterminado de 1.024.

El parámetro `Disk.MaxLUN` también determina cuántos LUN intentará detectar el código de análisis de SCSI mediante los comandos individuales de consulta INQUIRY si el destino SCSI no admite la detección directa mediante REPORT_LUNS.

Se puede modificar el parámetro `Disk.MaxLUN` según las necesidades. Por ejemplo, si su entorno tiene un número menor de dispositivos de almacenamiento con identificadores de LUN del 1 al 100, establezca el valor en 101. Como resultado, puede mejorar la velocidad de detección de dispositivos en destinos que no admiten REPORT_LUNS. Si se reduce el valor, se puede acortar el tiempo para volver a examinar y el tiempo de arranque. Sin embargo, el tiempo necesario para volver a examinar los dispositivos de almacenamiento también puede depender de otros factores, como el tipo de sistema de almacenamiento y la carga presente en el sistema de almacenamiento.

En otros casos, es posible que haya que aumentar el valor si el entorno utiliza identificadores de LUN mayores que 1023.

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Sistema**, haga clic en **Configuración avanzada del sistema**.
4. En la tabla Configuración avanzada del sistema, seleccione **Disk.MaxLUN** y haga clic en el icono **Editar**.
5. Cambie el valor actual por el valor de su elección y haga clic en **Aceptar**.

   El valor que introduzca especifica el identificador de LUN que viene después del último que desea detectar.

   Por ejemplo, para detectar identificadores de LUN del 1 al 100, establezca **Disk.MaxLUN** en 101.

Identificar problemas de conectividad del dispositivo

Cuando el host ESXi tiene un problema durante la conexión con un dispositivo de almacenamiento, el host trata el problema como permanente o temporal según ciertos factores.

Los problemas de conectividad de almacenamiento se producen por distintos motivos. Aunque ESXi no siempre puede determinar el motivo de la falta de disponibilidad de un dispositivo de almacenamiento o sus rutas de acceso, el host diferencia entre un estado de pérdida permanente de dispositivo (Permanent Device Loss, PDL) y un estado transitorio de todas las rutas de acceso inactivas (All Paths Down, APD) de almacenamiento.

pérdida permanente del dispositivo (Permanent Device Loss, PDL)

Una condición que se produce cuando un dispositivo de almacenamiento tiene errores permanentes o se elimina o excluye administrativamente. No se espera que vuelva a estar disponible. Cuando el dispositivo está permanentemente no disponible, ESXi recibe los códigos de detección apropiados o un rechazo de inicio de sesión por parte de las matrices de almacenamiento, y puede reconocer que el dispositivo se perdió de manera permanente.

Todas las rutas de acceso inactivas (All Paths Down, APD)

Una condición que se produce cuando un dispositivo de almacenamiento es inaccesible para el host y ninguna de las rutas de acceso al dispositivo está disponible. ESXi trata esto como una condición transitoria, ya que generalmente los problemas del dispositivo son temporales, y se espera que vuelva a estar disponible.

Problemas de conectividad y vSphere High Availability

Cuando el dispositivo entra en el estado PDL o APD, vSphere High Availability (HA) puede detectar problemas de conectividad y proporcionar una recuperación automatizada de las máquinas virtuales afectadas en el host ESXi. vSphere HA utiliza Protección de componentes de la máquina virtual (VM Component Protection, VMCP) para proteger las máquinas virtuales que se ejecutan en el host en el clúster de vSphere HA de errores de accesibilidad. Para obtener más información sobre VMCP y cómo configurar respuestas para los almacenes de datos y las máquinas virtuales cuando ocurre la condición de APD o PDL, consulte la documentación de *Disponibilidad de vSphere*.

Detectar condiciones de PDL

Se considera que un dispositivo de almacenamiento está en estado de pérdida permanente de dispositivo (Permanent Device Loss, PDL) cuando se vuelve no disponible de manera permanente para el host ESXi.

Por lo general, la condición de PDL se produce cuando un dispositivo se elimina sin intención o su identificador único cambia, o cuando el dispositivo tiene un error de hardware irrecuperable.

Cuando la matriz de almacenamiento determina que un dispositivo no está disponible de manera permanente, envía códigos de detección SCSI al host ESXi. Después de recibir los códigos de detección, el host reconoce que se han producido errores en el dispositivo y registra el estado del dispositivo como PDL. Para que el dispositivo se considere perdido de manera permanente, los códigos de detección se deben recibir en todas sus rutas.

Después de registrar el estado PDL del dispositivo, el host interrumpe los intentos que realiza para restablecer la conectividad o para enviar comandos al dispositivo.

vSphere Client muestra la siguiente información acerca del dispositivo:

- El estado operativo del dispositivo cambia a `Lost Communication`.
- Todas las rutas de acceso se muestran como `Dead`.
- Los almacenes de datos en el dispositivo no están disponibles.

Si no hay conexiones abiertas en el dispositivo o se cierran tras la última conexión, el host quita el dispositivo PDL y todas las rutas de acceso al dispositivo. Para deshabilitar la eliminación automática de rutas de acceso, establezca el parámetro avanzado `Disk.AutoremoveOnPDL` del host en 0.

Si el dispositivo regresa de la condición de PDL, el host puede detectarlo, pero lo trata como un dispositivo nuevo. No se garantiza la consistencia de los datos para las máquinas virtuales en el dispositivo recuperado.

Nota Cuando se produce un error en un dispositivo sin enviar los códigos de detección SCSI apropiados o un rechazo de inicio de sesión de iSCSI, el host no puede detectar las condiciones de PDL. En este caso, el host sigue tratando los problemas de conectividad del dispositivo como APD, incluso cuando los errores se producen de forma permanente en el dispositivo.

Pérdida permanente de dispositivo y códigos de detección SCSI

El siguiente ejemplo de código de detección SCSI de un registro del VMkernel indica que el dispositivo está en estado PDL.

```
H:0x0 D:0x2 P:0x0 Valid sense data: 0x5 0x25 0x0 or Logical Unit Not Supported
```

Pérdida permanente de dispositivo e iSCSI

En las matrices iSCSI con un solo LUN por destino, PDL se detecta a través de un error en el inicio de sesión iSCSI. Una matriz de almacenamiento iSCSI rechaza el intento del host de iniciar una sesión iSCSI con el motivo `Target Unavailable` (Destino no disponible). Como sucede con los códigos de detección, esta respuesta debe recibirse en todas las rutas de acceso para que el dispositivo se considere perdido de manera permanente.

Pérdida permanente de dispositivo y máquinas virtuales

Después de registrar el estado PDL del dispositivo, el host cierra todas las operaciones de E/S de las máquinas virtuales. vSphere HA puede detectar el estado PDL y reiniciar las máquinas virtuales que tengan errores.

Eliminar dispositivo de almacenamiento planificada

Cuando un dispositivo de almacenamiento funciona mal, puede evitar la condición de pérdida de dispositivo permanente (Permanent Device Loss, PDL) o todas las rutas de acceso inactivas (All Paths Down, APD). Quite y vuelva a conectar de forma planificada el dispositivo de almacenamiento.

La eliminación del dispositivo planificada es una desconexión intencional de un dispositivo de almacenamiento. También es posible que planifique quitar un dispositivo por motivos como la actualización de hardware o la reconfiguración de los dispositivos de almacenamiento. Cuando se realiza una eliminación y reconexión ordenada de un dispositivo de almacenamiento, se completan varias tareas.

Tarea	Descripción
Migre las máquinas virtuales del dispositivo que planifica separar.	*Administrar vCenter Server y hosts*
Desmonte el almacén de datos implementado en el dispositivo.	Consulte Desmontar almacenes de datos.

Tarea	Descripción
Separe el dispositivo de almacenamiento.	Consulte Separar dispositivos de almacenamiento.
En el caso de un dispositivo iSCSI con un solo LUN por destino, elimine la entrada de destino estático de cada HBA de iSCSI que tenga una ruta de acceso al dispositivo de almacenamiento.	Consulte Quitar destinos iSCSI dinámicos o estáticos.
Realice cualquier reconfiguración necesaria del dispositivo de almacenamiento con la consola matriz.	Consulte la documentación del proveedor.
Vuelva a conectar el dispositivo de almacenamiento.	Consulte Asociar dispositivos de almacenamiento.
Monte el almacén de datos y reinicie las máquinas virtuales.	Consulte Montar almacenes de datos.

Separar dispositivos de almacenamiento

Desconecte de forma segura un dispositivo de almacenamiento del host ESXi.

Es posible que se deba desconectar el dispositivo para que el host no pueda acceder cuando, por ejemplo, se realice una actualización de hardware del lado del almacenamiento.

Requisitos previos

- El dispositivo no contiene ningún almacén de datos.
- Ninguna máquina virtual usa el dispositivo como disco RDM.
- El dispositivo no contiene una partición de diagnóstico o una partición desde cero.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Dispositivos de almacenamiento**.

4 Seleccione el dispositivo que desea desconectar y haga clic en el icono **Desconectar**.

Resultados

El dispositivo deja de ser accesible. El estado operativo del dispositivo cambia a Desmontado.

Pasos siguientes

Si varios hosts comparten el dispositivo, desconecte el dispositivo de cada host.

Asociar dispositivos de almacenamiento

Vuelva a asociar un dispositivo de almacenamiento que desasoció anteriormente del host ESXi.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Dispositivos de almacenamiento**.

4 Seleccione el dispositivo de almacenamiento desconectado y haga clic en el icono **Conectar**.

Resultados

El dispositivo vuelve a ser accesible.

Recuperación de condiciones de PDL

Una condición de pérdida permanente de dispositivo (Permanent Device Loss, PDL) no planificada ocurre cuando un dispositivo de almacenamiento deja de estar disponible permanentemente sin desconectarlo adecuadamente del host ESXi.

Los elementos siguientes en vSphere Client indican que el dispositivo está en estado de PDL:

- El almacén de datos implementado en el dispositivo no está disponible.
- El estado operativo del dispositivo cambia a Comunicación perdida.
- Todas las rutas de acceso aparecen como Inactivas.
- En el archivo de registro VMkernel aparece una advertencia acerca de que el dispositivo se encuentra inaccesible permanentemente.

Para recuperarse de la condición de PDL no planificada y quitar el dispositivo no disponible del host, realice las siguientes tareas.

Tarea	Descripción
Apague y cancele el registro de todas las máquinas virtuales que están en ejecución en los almacenes de datos afectados por la condición de PDL.	Consulte *Administrar máquinas virtuales de vSphere*.
Desmonte el almacén de datos.	Consulte Desmontar almacenes de datos.
Vuelva a examinar todos los hosts ESXi que tenían acceso al dispositivo. **Nota** Si el proceso de volver a examinar no se completa correctamente y el host sigue mostrando el dispositivo, es posible que aún existan algunas operaciones de E/S pendientes o referencias activas al dispositivo. Busque elementos que aún puedan tener referencias activas al dispositivo o al almacén de datos. Los elementos incluyen las máquinas virtuales, las plantillas, las imágenes ISO, las asignaciones de dispositivos sin formato, etc.	Consulte Realizar la operación para volver a examinar el almacenamiento.

Manejar condiciones de APD transitorias

Se considera que un dispositivo de almacenamiento se encuentra en el estado con todas las rutas de acceso inactivas (All Paths Down, APD) cuando no está disponible para el host ESXi durante un período de tiempo indeterminado.

Los motivos de un estado APD pueden ser, por ejemplo, un conmutador con errores o un cable de almacenamiento desconectado.

A diferencia del estado de pérdida de dispositivo permanente (Permanent Device Loss, PDL), el host considera que el estado APD es transitorio y espera que el dispositivo esté nuevamente disponible.

El host vuelve a intentar los comandos emitidos con el fin de restablecer la conectividad con el dispositivo. Si los comandos del host siguen intentándolo sin éxito durante un período de tiempo prolongado, el host podría sufrir otros problemas de rendimiento. En ese caso el host y sus máquinas virtuales también podrían dejar de responder.

Para evitar estos problemas, el host utiliza la característica de manejo de APD predeterminada. Cuando un dispositivo entra en estado APD, el host se convierte en un temporizador. Con el temporizador activado, el host sigue reintentando los comandos que no son de máquina virtual solo durante un período de tiempo limitado.

De forma predeterminada, el tiempo de espera de APD se establece en 140 segundos. Este valor es, por lo general, superior al que necesita la mayoría de los dispositivos para recuperarse ante una pérdida de conexión. Si el dispositivo vuelve a estar disponible en este lapso, el host y su máquina virtual seguirán ejecutándose sin experimentar ningún problema.

Si el dispositivo no se recupera y se cumple el tiempo de espera, el host detiene sus intentos y todas las E/S de máquinas no virtuales. Las E/S de máquinas virtuales seguirán reintentándose. vSphere Client muestra la siguiente información del dispositivo con el tiempo de espera de APD cumplido:

- El estado operativo del dispositivo cambia a `Dead or Error`.
- Todas las rutas de acceso se muestran como `Dead`.
- Los almacenes de datos en el dispositivo se atenúan.

Aunque el dispositivo y los almacenes de datos no están disponibles, las máquinas virtuales siguen respondiendo. Puede apagar las máquinas virtuales o migrarlas a otro almacén de datos o host.

Si las rutas del dispositivo vuelven a funcionar más adelante, el host puede reanudar las E/S hacia el dispositivo y terminar el tratamiento especial de APD.

Deshabilitar el manejo de APD de almacenamiento

El manejo de todas las rutas de acceso inactivas (All Paths Down, APD) de almacenamiento en el host ESXi está habilitado de manera predeterminada. Cuando está habilitado, el host continúa reintentando la ejecución de comandos de E/S de máquinas no virtuales en un dispositivo de almacenamiento en estado APD durante un período limitado. Cuando caduca este período, el host interrumpe los reintentos y finaliza todas las operaciones de E/S de las máquinas no virtuales. Es posible deshabilitar la característica de manejo de APD en el host.

Si se deshabilita el manejo de APD, el host continúa reintentando la ejecución de los comandos emitidos indefinidamente, con la intención de volver a conectarse con el dispositivo APD. Esto puede causar que las máquinas virtuales en el host superen su tiempo de espera de E/S interno y dejen de responder o generen errores. El host podría desconectarse de vCenter Server.

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Sistema**, haga clic en **Configuración avanzada del sistema**.
4. En la tabla Configuración avanzada del sistema, seleccione el parámetro **Misc.APDHandlingEnable** y haga clic en el icono `Edit`.
5. Cambie el valor a 0.

Resultados

Si deshabilitó el manejo de APD, puede volver a habilitarlo y establecer su valor en 1 cuando un dispositivo entre al estado APD. La característica de manejo de APD interna se activa inmediatamente, y el temporizador se inicia con el valor de tiempo de espera actual para cada dispositivo en APD.

Cambiar los límites de tiempo de espera para APD de almacenamiento

El parámetro de tiempo de espera controla durante cuántos segundos el host ESXi debe reintentar los comandos de E/S en un dispositivo de almacenamiento que se encuentra en el estado APD, con todas las rutas de acceso inactivas. Puede cambiar el valor de tiempo de espera predeterminado.

El período de tiempo de espera se inicia inmediatamente después de que el dispositivo entra en el estado APD. Una vez finalizado el tiempo de espera, el host marca el dispositivo en estado APD como inaccesible. El host deja de reintentar cualquier E/S que no provenga de las máquinas virtuales. El host sigue intentando la E/S de la máquina virtual.

De manera predeterminada, el parámetro de tiempo de espera en el host se establece en 140 segundos. Puede aumentar el valor del tiempo de espera si, por ejemplo, los dispositivos de almacenamiento conectados al host ESXi tardan más de 140 segundos en recuperarse de una pérdida de conexión.

Nota Si cambia el parámetro de tiempo de espera después de que el dispositivo deja de estar disponible, el cambio no tiene efecto para ese incidente de APD en particular.

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Sistema**, haga clic en **Configuración avanzada del sistema**.
4. En la tabla Configuración avanzada del sistema, seleccione el parámetro **Misc.APDTimeout** y haga clic en el icono `Edit`.
5. Cambie el valor predeterminado.

   Puede introducir un valor entre 20 y 99999 segundos.

Comprobar el estado de conexión de un dispositivo de almacenamiento en el host ESXi

Use el comando `esxcli` para comprobar el estado de conexión de un dispositivo de almacenamiento en particular.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1. Ejecute el comando **`esxcli storage core device list -d=`*`device_ID`***.
2. Revise el estado de la conexión en el área `Status:`.
   - `on`: el dispositivo está conectado.
   - `dead`: el dispositivo entró al estado APD. Se inicia el temporizador de APD.
   - `dead timeout`: caducó el tiempo de espera de APD.
   - `not connected`: el dispositivo está en estado PDL.

Habilitar o deshabilitar el LED de ubicación en dispositivos de almacenamiento ESXi

Utilice el LED localizador para identificar dispositivos de almacenamiento específicos y poder reconocerlos entre otros dispositivos. Es posible encender o apagar el LED localizador.

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Almacenamiento**, haga clic en **Dispositivos de almacenamiento**.
4. En la lista de dispositivos de almacenamiento, seleccione uno o varios discos y habilite o deshabilite el indicador del LED localizador.

Opción	Descripción
Habilitar	Haga clic en el icono **Encender LED**.
Deshabilitar	Haga clic en el icono **Apagar LED**.

Borrar dispositivos de almacenamiento

Algunas funcionalidades, como vSAN o el recurso flash virtual, requieren que el host ESXi utilice dispositivos de almacenamiento limpios. Puede borrar una unidad HHD o un dispositivo flash, y eliminar todos sus datos existentes.

Requisitos previos

- Asegúrese de que el host esté conectado.
- Compruebe que los dispositivos que planea borrar no estén en uso.
- Privilegio necesario: **Host.Config.Storage**

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Almacenamiento**, haga clic en **Dispositivos de almacenamiento**.
4. Seleccione uno o varios dispositivos, y haga clic en el icono **Borrar particiones**.
5. Compruebe que la información de partición que borrará no es crítica.
6. Haga clic en **Aceptar** para confirmar el cambio.

Cambiar los ajustes de reserva perenne

Puede ajustar la configuración de reserva perenne en los dispositivos de almacenamiento que se utilizan como asignaciones de dispositivos sin formato (Raw Device Mappings, RDM) físicas en las configuraciones de clústeres de conmutación por error de Windows Server (Windows Server Failover Clustering, WSFC).

Los nodos del clúster de WSFC que se propagan por varios hosts ESXi requieren RDM físicas. Las RDM se comparten entre todos los hosts en los que se ejecutan nodos del clúster. El host con el nodo activo contiene reservas de SCSI-3 persistentes en todos los dispositivos de RDM compartidos. Cuando el nodo activo está en ejecución y los dispositivos están bloqueados, ningún otro host puede escribir en los dispositivos. Si otro host participante arranca mientras el nodo activo mantiene el bloqueo en los dispositivos, el arranque puede tardar mucho tiempo, ya que el host intenta sin éxito ponerse en contacto con los dispositivos bloqueados. El mismo problema también puede afectar a las operaciones de reexaminación.

Para evitar este problema, active la reserva perenne para todos los dispositivos en los hosts ESXi en los que residen los nodos de WSFC secundarios con RDM. Este ajuste informa al host ESXi sobre la reserva de SCSI permanente en los dispositivos, de modo que el host pueda omitir los dispositivos durante el proceso de reexaminación de arranque o almacenamiento.

Si más adelante desea volver a utilizar los dispositivos marcados como almacenes de datos de VMFS, elimine la reserva para evitar comportamientos impredecibles del almacén de datos.

Para obtener información acerca de los clústeres de WSFC, consulte la documentación de *Configuración de clústeres de conmutación por error de Windows Server*.

Requisitos previos

Antes de marcar un dispositivo como reservado de forma perenne, asegúrese de que el dispositivo no contenga un almacén de datos de VMFS.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Dispositivos de almacenamiento**.

4 Seleccione el dispositivo de almacenamiento de la lista y haga clic en uno de los siguientes iconos.

Opción	Descripción
Marcar como reservado de forma perenne	Marque el dispositivo seleccionado como reservado de forma perenne. **Nota** Repita el procedimiento para cada dispositivo RDM que participe en el clúster de WSFC.
Desmarcar como reservado de forma perenne	Borre la reserva perenne para el dispositivo que se marcó previamente.

Resultados

La configuración se almacena de forma permanente con el host ESXi y persiste durante los reinicios.

Ejemplo

También puede utilizar el comando `esxcli` para marcar los dispositivos que participan en el clúster de WSFC.

1 Marque los dispositivos como reservados de forma perenne.

```
esxcli storage core device setconfig -d naa.id --perennially-reserved=true
```

2 Compruebe que el dispositivo esté reservado de forma perenne.

```
esxcli storage core device list -d naa.id
```

En la salida del comando `esxcli`, busque la entrada `Is Perennially Reserved: true`.

3 Para eliminar la marca de reserva perenne, ejecute el siguiente comando.

```
esxcli storage core device setconfig -d naa.id --perennially-reserved=false
```

Trabajar con dispositivos flash 15

Además de las unidades de disco duro (Hard Disk Drives, HDD) de almacenamiento normales, ESXi es compatible con dispositivos de almacenamiento flash.

A diferencia de los HDD normales que son dispositivos electromecánicos que contienen partes móviles, los dispositivos flash utilizan semiconductores como medio de almacenamiento y no tienen partes móviles. Por lo general, los dispositivos flash son resistentes y proporcionan un acceso más rápido a los datos.

Para detectar dispositivos flash, ESXi utiliza un mecanismo de consulta basado en estándares T10. Compruebe con el proveedor si la matriz de almacenamiento es compatible con el mecanismo de ESXi de detección de dispositivos flash.

Una vez que el host detecta los dispositivos flash, es posible utilizarlos para varias tareas y funcionalidades.

Si utiliza almacenamiento de NVMe, habilite el complemento de rendimiento alto (HPP) para mejorar el rendimiento del almacenamiento. Consulte Complemento de alto rendimiento de VMware y esquemas de selección de rutas de acceso.

Para obtener información específica sobre el uso del almacenamiento de NVMe con ESXi, consulte Capítulo 16 Acerca del almacenamiento de NVMe de VMware.

Tabla 15-1. Usar dispositivos flash con ESXi

Funcionalidad	Descripción
vSAN	vSAN requiere dispositivos flash. Para obtener más información, consulte la documentación sobre *Administrar VMware vSAN*.
Almacenes de datos de VMFS	Cree almacenes de datos de VMFS en dispositivos flash. Use los almacenes de datos con los siguientes propósitos: ■ Almacenar máquinas virtuales. Algunos sistemas operativos invitados pueden identificar discos virtuales almacenados en estos almacenes de datos como discos virtuales flash. ■ Asigne espacio del almacén de datos para la memoria caché de intercambio del host ESXi. Consulte Configurar la memoria caché del host con un almacén de datos de VMFS.
Recurso flash virtual (VFFS)	Si el proveedor lo solicita, configure un recurso flash virtual y úselo para los filtros de E/S de almacenamiento en caché. Consulte Capítulo 23 Filtrar E/S de máquinas virtuales.

Dispositivos flash y máquinas virtuales

Los sistemas operativos invitados pueden identificar discos virtuales que residen en almacenes de datos basados en flash como discos virtuales flash.

Los sistemas operativos invitados pueden usar comandos de consulta estándares como SCSI VPD Page (B1h) para dispositivos SCSI y ATA IDENTIFY DEVICE (Word 217) para dispositivos IDE.

Para los clones asociados, las snapshots nativas y los discos delta, los comandos de consulta informan del estado de flash virtual del disco base.

Los sistemas operativos pueden detectar que un disco virtual es un disco flash en las siguientes condiciones:

- La detección de discos virtuales flash se admite en máquinas virtuales y hardware virtual de la versión 8 o posterior.
- Los dispositivos que respaldan un almacén de datos de VMFS compartido deben marcarse como Flash en todos los hosts.
- Si el almacén de datos de VMFS incluye varias extensiones de dispositivos, todas las extensiones físicas subyacentes deben estar basadas en flash.

Este capítulo incluye los siguientes temas:

Marcado de dispositivos de almacenamiento

Puede marcar dispositivos de almacenamiento en un host ESXi como dispositivos flash locales.

Cuando se configura vSAN o un recurso de flash virtual, el entorno de almacenamiento debe incluir dispositivos flash locales.

Sin embargo, ESXi no puede reconocer ciertos dispositivos de almacenamiento como dispositivos flash si los proveedores no incluyen compatibilidad con la detección automática de dispositivos flash. En otros casos, es posible que algunos dispositivos no se detecten como locales, y ESXi los marca como remotos. Cuando los dispositivos no se reconocen como dispositivos flash locales, se excluyen de la lista de dispositivos ofrecidos para vSAN o el recurso flash virtual. Si se marcan estos dispositivos como flash locales, estarán disponibles para vSAN y el recurso flash virtual.

Marcar dispositivos de almacenamiento como flash

Si ESXi no reconoce los dispositivos como flash, márquelos como dispositivos flash.

ESXi no reconoce ciertos dispositivos como flash cuando los proveedores no admiten la detección automática de discos flash. La columna Tipo de unidad de los dispositivos muestra HDD como el tipo.

Precaución Marcar los dispositivos HDD como flash puede deteriorar el rendimiento de los almacenes de datos y los servicios que los utilizan. Marque los dispositivos únicamente si tiene certeza de que son dispositivos flash.

Requisitos previos

Compruebe que el dispositivo no esté en uso.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Dispositivos de almacenamiento**.

4 En la lista de dispositivos de almacenamiento, seleccione uno o varios dispositivos HDD y haga clic en **Marcar como discos flash** ().

5 Haga clic en **Sí** para guardar los cambios.

Resultados

El tipo de dispositivo cambia a flash.

Pasos siguientes

Si el dispositivo flash que marca se comparte entre varios hosts, asegúrese de marcar el dispositivo en todos los hosts que comparten el dispositivo.

Marcar dispositivos de almacenamiento como locales

ESXi permite marcar dispositivos como locales. Esta acción es útil en los casos en que ESXi no puede determinar si ciertos dispositivos son locales.

Requisitos previos

- Asegúrese de que el dispositivo no esté compartido.
- Apague las máquinas virtuales que residen en ese dispositivo y desmonte los almacenes de datos asociados.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Dispositivos de almacenamiento**.

4 En la lista de dispositivos de almacenamiento, seleccione uno o varios dispositivos remotos y haga clic en el icono **Marcar como local**.

5 Haga clic en **Sí** para guardar los cambios.

Supervisar dispositivos flash

Puede supervisar ciertos parámetros de los dispositivos flash críticos, incluidos `Media Wearout Indicator`, `Temperature` y `Reallocated Sector Count` desde un host ESXi.

Use el comando `esxcli` para supervisar dispositivos flash.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

◆ Muestre las estadísticas de los dispositivos flash mediante la ejecución del siguiente comando:

`esxcli storage core device smart get -d=`*`flash device_ID`*

Prácticas recomendadas para dispositivos flash

Siga estas prácticas recomendadas al utilizar dispositivos flash en el entorno de vSphere.

- Utilice los dispositivos flash aprobados por la *guía de compatibilidad de VMware*.
- Asegúrese de utilizar el firmware más reciente con dispositivos flash. Consulte con frecuencia a los proveedores de almacenamiento para saber si existen actualizaciones.
- Supervise con atención la intensidad con que utiliza el dispositivo flash y calcule su vida útil estimada. La expectativa de vida útil depende de qué tan activamente siga utilizando el dispositivo flash. Consulte Vida útil estimada para dispositivos flash.
- Si utiliza dispositivos NVMe para almacenamiento, habilite el complemento de rendimiento alto (high-performance plug-in, HPP) para mejorar el rendimiento del almacenamiento. Para obtener información específica sobre el uso de los dispositivos NVMe, consulte Complemento de alto rendimiento de VMware y esquemas de selección de rutas de acceso.

Vida útil estimada para dispositivos flash

Al trabajar con dispositivos flash, supervise qué tan activamente los utiliza y calcule su duración estimada.

Por lo general, los proveedores de almacenamiento proporcionan estimaciones de duración confiables para un dispositivo flash en condiciones ideales. Por ejemplo, un proveedor puede garantizar una duración de 5 años en condiciones de 20 GB de escritura por día. Sin embargo, la expectativa de vida útil más realista del dispositivo depende de cuántas escrituras genera realmente el host ESXi por día. Siga estos pasos para calcular la duración del dispositivo flash.

Requisitos previos

Tenga en cuenta la cantidad de días que transcurrieron desde el último reinicio del host ESXi. Por ejemplo, diez días.

Procedimiento

1 Obtenga el número total de bloques escritos en el dispositivo flash desde el último reinicio.

Ejecute el comando **esxcli storage core device stats get -d=*device_ID***. Por ejemplo:

```
~ # esxcli storage core device stats get -d t10.xxxxxxxxxxxxxxx
    Device: t10.xxxxxxxxxxxxxxx
    Successful Commands: xxxxxxx
    Blocks Read: xxxxxxxx
    Blocks Written: 629145600
    Read Operations: xxxxxxxx
```

El elemento "Blocks Written" muestra el número de bloques escritos en el dispositivo desde el último reinicio. En este ejemplo, el valor es 629.145.600. Después de cada reinicio, se restablece en 0.

2 Calcule el número total de escrituras y conviértalo a GB.

Un bloque tiene 512 bytes. Para calcular el número total de escrituras, multiplique el valor de "Blocks Written" por 512 y convierta el valor resultante a GB.

En este ejemplo, el número total de escrituras desde el último reinicio es de aproximadamente 322 GB.

3 Calcule el número promedio de escrituras por día en GB.

Divida el número total de escrituras por el número de días transcurridos desde el último reinicio.

Si el último reinicio fue hace diez días, el resultado es 32 GB de escrituras por día. Puede promediar este número para un período determinado..

4 Haga una estimación de la duración del dispositivo con la fórmula siguiente:

vendor provided number of writes per day multiplicado por *vendor provided life span* dividido por *actual average number of writes per day*

Por ejemplo, si el proveedor garantiza una duración de 5 años con 20 GB de escritura diarios y la cantidad de escrituras diarias real es de 30 GB, la duración del dispositivo flash será de aproximadamente 3,3 años.

Acerca del recurso flash virtual

Puede combinar dispositivos flash locales en un host ESXi en una única capa de almacenamiento en caché virtualizada denominada recurso flash virtual.

Cuando se configura el recurso flash virtual, se crea un sistema de archivos nuevo: el sistema de archivos flash virtual (VFFS). VFFS deriva de VMFS, que está optimizado para dispositivos flash y se usa para agrupar los dispositivos flash físicos en un grupo único de recursos de almacenamiento en caché. Como recurso no persistente, no puede usarse para almacenar máquinas virtuales.

Después de configurar el recurso flash virtual, se puede usar en los filtros de E/S de almacenamiento en caché. Consulte Capítulo 23 Filtrar E/S de máquinas virtuales.

Consideraciones sobre el recurso flash virtual

Al configurar un recurso flash virtual, se aplican varias consideraciones.

- Se puede tener un solo recurso flash virtual en un solo host ESXi. El recurso flash virtual se administra solo en el nivel del host.
- El recurso flash virtual no se puede utilizar para almacenar máquinas virtuales. El recurso flash virtual es solo una capa de almacenamiento en caché.
- Solo es posible utilizar dispositivos flash locales para el recurso flash virtual.
- Puede crear el recurso flash virtual desde dispositivos flash combinados. Todos los tipos de dispositivos se tratan del mismo modo, y no se realiza distinción entre la conectividad SAS, SATA ni PCI Express. Al crear el recurso desde dispositivos flash combinados, asegúrese de agrupar los dispositivos de rendimiento similar para maximizar el rendimiento.
- No se pueden utilizar los mismos dispositivos flash para el recurso flash virtual y vSAN. Cada uno requiere su propio dispositivo flash dedicado y exclusivo.

Configurar un recurso flash virtual

Puede configurar un recurso flash virtual o agregar capacidad a un recurso flash virtual existente.

Para configurar un recurso flash virtual, se deben utilizar dispositivos flash locales conectados al host o al clúster de hosts. Para aumentar la capacidad del recurso flash virtual, es posible agregar más dispositivos, hasta la cantidad máxima indicada en la documentación de *Máximos de configuración*. Un dispositivo flash individual debe estar asignado exclusivamente al recurso flash virtual. Ninguna otra funcionalidad de vSphere, como vSAN o VMFS, puede compartir el dispositivo con el recurso flash virtual.

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Flash virtual**, haga clic en **Administración de recursos flash virtuales**.

4 Haga clic en una de las siguientes opciones.

Opción	Descripción
Agregar capacidad	Si crea el recurso flash virtual en un host individual.
Agregar capacidad al clúster	Si crea el recurso flash virtual en un clúster.

5 En la lista de entidades disponibles, seleccione una o más entidades que desee usar para el recurso flash virtual y haga clic en **Aceptar**.

Si los dispositivos flash no aparecen en la lista, consulte Marcado de dispositivos de almacenamiento.

Opción	Descripción
Disco local de VMware	Seleccione cualquier combinación de dispositivos flash no reclamados. ESXi crea el volumen VFFS en uno de los dispositivos y, a continuación, extiende el volumen al resto de los dispositivos. El sistema configura el recurso flash virtual en el volumen VFFS completo. Si existe un volumen VFFS en el host, no puede seleccionar ningún dispositivo no reclamado sin seleccionar primero el volumen VFFS existente.
***ID del volumen*: configurar con las extensiones de volumen VFFS existentes**	Si creó previamente un volumen VFFS en uno de los dispositivos flash del host mediante el comando `vmkfstools`, el volumen también aparece en la lista de entidades que cumplen los requisitos. Puede seleccionar solo este volumen para el recurso flash virtual. O combínelo con los dispositivos no reclamados. ESXi usa el volumen VFFS existente para extenderlo a otros dispositivos.

Resultados

Se crea el recurso flash virtual. El área Copia de seguridad de los dispositivos enumera todos los dispositivos que se utilizan para el recurso flash virtual.

Pasos siguientes

Utilice el recurso flash virtual para los filtros de almacenamiento en caché de E/S desarrollados mediante las API de vSphere para el filtrado de E/S. Consulte Utilizar dispositivos de almacenamiento flash con filtros de E/S de memoria caché.

Para aumentar la capacidad, agregue más dispositivos flash al recurso flash virtual.

Quitar el recurso flash virtual

Es posible que deba quitar un recurso flash virtual implementado en dispositivos flash locales conectados al host ESXi. Al quitar el recurso flash virtual, se liberan los dispositivos para otros servicios.

Requisitos previos

- Compruebe que el recurso flash virtual no se utilice para los filtros de E/S.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Flash virtual**, haga clic en **Administración de recursos flash virtuales** y haga clic en **Quitar todo**.

Resultados

Después de quitar el recurso flash virtual y borrar el dispositivo flash, el dispositivo estará disponible para otras operaciones.

Establecer una alarma para el uso de flash virtual

Establezca una alarma para indicar el momento en que el uso de un recurso de flash virtual en el host ESXi supera el umbral especificado.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Sistema**, haga clic en **Configuración avanzada del sistema**.

4 Seleccione la configuración que desea cambiar y haga clic en el botón **Editar**.

Parámetro	Descripción
VFLASH.ResourceUsageThreshold	El sistema activa la alarma `Host vFlash resource usage` cuando el uso de un recurso de flash virtual supera el umbral. El umbral predeterminado es del 80 %. Puede cambiar este umbral a un valor apropiado. La alarma se borra cuando el uso del recurso flash virtual cae por debajo del umbral.

5 Haga clic en **Aceptar**.

Configurar la memoria caché del host con un almacén de datos de VMFS

Habilite el host ESXi para el intercambio con la memoria caché del host. También puede cambiar la cantidad de espacio asignado para la memoria caché del host.

Los hosts ESXi pueden utilizar una parte de una entidad de almacenamiento respaldada por flash como memoria caché de intercambio compartida por todas las máquinas virtuales.

La memoria caché en el nivel del host está compuesta por archivos en un disco de latencia baja que ESXi utiliza como memoria caché con reescritura para archivos de intercambio de máquinas virtuales. Todas las máquinas virtuales que se ejecutan en el host comparten la memoria caché. El intercambio en el nivel del host de páginas de máquinas virtuales aprovecha al máximo el espacio de dispositivos flash potencialmente limitado.

Requisitos previos

Cree un almacén de datos de VMFS con dispositivos flash como respaldo. Consulte Crear un almacén de datos de VMFS.

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Almacenamiento**, haga clic en **Configuración de caché del host**.
4. Seleccione el almacén de datos flash en la lista y haga clic en el icono **Editar**.
5. Asigne el espacio adecuado para la memoria caché del host.
6. Haga clic en **Aceptar**.

Mantener los discos flash sin VMFS

Si se usa la opción de arranque con creación automática de particiones al instalar o implementar de forma automática ESXi, la opción de partición automática crea un almacén de datos de VMFS en el almacenamiento local del host. En algunos casos, es necesario mantener los discos flash del almacenamiento local sin formato.

Problema

De forma predeterminada, la creación automática de particiones implementa sistemas de archivos de VMFS en cualquier disco de almacenamiento local sin usar en su host, incluidos discos flash.

Sin embargo, un disco flash formateado con VMFS queda no disponible para funciones como disco flash virtual y vSAN. Ambas funciones requieren un disco flash sin formato y tampoco pueden compartir el disco con otro sistema de archivos.

Solución

Para asegurar que la creación automática de particiones no formatee el disco flash con VMFS, use las siguientes opciones de arranque al instalar ESXi o arrancar el host ESXi por primera vez:

- **`autoPartition=TRUE`**
- **`skipPartitioningSsds=TRUE`**

Si utiliza Auto Deploy, configure estos parámetros en un host ESXi de referencia.

1. En vSphere Client, desplácese al host que planea usar como el host de referencia y haga clic en la pestaña **Configurar**.
2. Haga clic en **Sistema** para abrir las opciones del sistema y haga clic en **Configuración avanzada del sistema**.

3 Establezca los siguientes elementos.

Parámetro	Valor
VMkernel.Boot.autoPartition	True
VMkernel.Boot.skipPartitioningSsds	True

4 Reinicie el host.

Si los discos flash que planea usar con el recurso de flash virtual y vSAN ya tienen almacenes de datos de VMFS, elimine los almacenes de datos.

Acerca del almacenamiento de NVMe de VMware

16

Los dispositivos de almacenamiento de memoria no volátil (NVM) que utilizan memoria persistente son cada vez más populares en los centros de datos. NVM Express (NVMe) es un protocolo estandarizado que se diseñó específicamente para la comunicación de varias colas y alto rendimiento con dispositivos NVM. ESXi es compatible con el protocolo NVMe para conectarse a dispositivos de almacenamiento en red y locales.

Este capítulo incluye los siguientes temas:

Conceptos de NVMe de VMware

Antes de comenzar a trabajar con el almacenamiento de NVMe en el entorno ESXi, puede familiarizarse con los conceptos básicos de NVMe.

NVM Express (NVMe)

NVMe es un método para conectar y transferir datos entre un host y un sistema de almacenamiento de destino. Está diseñado para usarse con soportes de almacenamiento más rápidos equipados con memoria no volátil, como dispositivos flash. Este tipo de almacenamiento puede alcanzar una latencia baja, un uso de CPU bajo y un alto rendimiento. Además, por lo general, sirve como alternativa al almacenamiento SCSI.

Transportes NVMe

El almacenamiento de NVMe se puede asociar directamente a un host mediante una interfaz PCIe o indirectamente a través de diferentes transportes de tejido. VMware NVMe over Fabrics (NVMe-oF) proporciona una conectividad a distancia entre un host y un dispositivo de almacenamiento de destino en una matriz de almacenamiento compartido.

Actualmente existen los siguientes tipos de transportes para NVMe. Para obtener más información, consulte Requisitos y limitaciones del almacenamiento de NVMe de VMware.

Transporte NVMe	Compatibilidad con ESXi
NVMe over PCIe	Almacenamiento local.
NVMe over RDMA	Almacenamiento de NVMe-oF compartido. Con la tecnología RoCE V2.
NVMe over Fibre Channel (FC-NVMe)	Almacenamiento de NVMe-oF compartido.
NVME over TCP	Almacenamiento de NVMe-oF compartido.

Espacios de nombres de NVMe

En la matriz de almacenamiento de NVMe, un espacio de nombres es un volumen de almacenamiento respaldado por cierta cantidad de memoria no volátil. En el contexto de ESXi, el espacio de nombres es análogo a un dispositivo de almacenamiento o LUN. Una vez que el host ESXi detecta el espacio de nombres de NVMe, aparece un dispositivo flash que representa el espacio de nombres en la lista de dispositivos de almacenamiento en vSphere Client. Puede utilizar el dispositivo para crear un almacén de datos de VMFS y almacenar máquinas virtuales.

Controladores de NVMe

Un controlador está asociado a uno o varios espacios de nombres de NVMe y proporciona una ruta de acceso entre el host ESXi y los espacios de nombres de la matriz de almacenamiento. Para acceder al controlador, el host puede utilizar dos mecanismos, la detección del controlador y la conexión del controlador. Para obtener información, consulte Agregar controlador para NVMe over Fabrics.

Detección del controlador

Con este mecanismo, el host ESXi primero se contacta con un controlador de detección. El controlador de detección devuelve una lista de los controladores disponibles. Después de seleccionar un controlador para que el host acceda, todos los espacios de nombres asociados con este controlador pasan a estar disponibles para el host.

Conexión de controladores

Su host ESXi se conecta al controlador que especifique. Todos los espacios de nombres asociados con este controlador pasan a estar disponibles para el host.

Subsistema de NVMe

Por lo general, un subsistema de NVMe es una matriz de almacenamiento que puede incluir varios controladores de NVMe, varios espacios de nombres, un medio de almacenamiento de memoria no volátil y una interfaz entre el controlador y el medio de almacenamiento de memoria no volátil. El subsistema se identifica con un nombre calificado de NVMe (NVMe Qualified Name, NQN) del subsistema.

Complemento de alto rendimiento (High-Performance Plug-in, HPP) de VMware

De forma predeterminada, el host ESXi utiliza HPP para reclamar los destinos de NVMe. Al seleccionar rutas de acceso físicas para solicitudes de E/S, HPP aplica un esquema de selección de rutas de acceso (PSS) adecuado. Para obtener información sobre HPP, consulte Complemento de alto rendimiento de VMware y esquemas de selección de rutas de acceso. Para cambiar el mecanismo de selección de la ruta de acceso predeterminada, consulte Cambiar la directiva de selección de rutas de acceso.

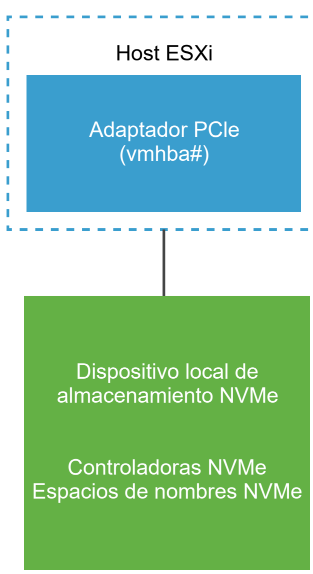
Arquitectura y componentes básicos de VMware NVMe

ESXi admite el almacenamiento de NVMe over PCIe local y el almacenamiento compartido NVMe-oF, como NVMe over Fibre Channel y NVMe over RDMA (RoCE V2) o NVMe over TCP.

En los entornos de NVMe, los destinos pueden presentar espacios de nombres, equivalentes a los LUN en SCSI, a un host en los modos de acceso asimétrico o activo/activo. ESXi puede detectar y utilizar los espacios de nombres presentados de cualquiera de las dos formas. ESXi emula internamente los destinos de NVMe-oF como destinos SCSI y los presenta como destinos SCSI activos/activos o destinos SCSI implícitos de ALUA.

VMware NVMe over PCIe

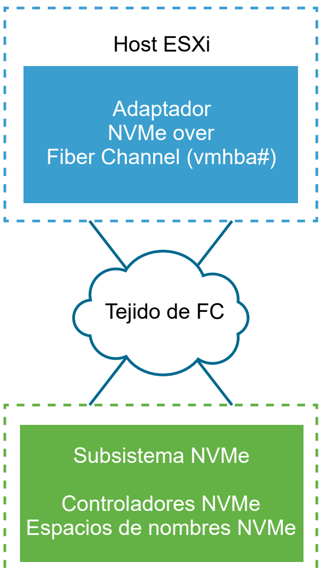
En esta configuración, el host ESXi usa un adaptador de almacenamiento de PCIe para acceder a uno o varios dispositivos de almacenamiento de NVMe locales. Después de instalar el adaptador en el host, este detecta los dispositivos NVMe disponibles y aparecen en la lista de dispositivos de almacenamiento en vSphere Client.



VMware NVMe over FC

Esta tecnología asigna NVMe al protocolo de Fibre Channel para habilitar la transferencia de datos y comandos entre un equipo host y un dispositivo de almacenamiento de destino. Este transporte puede utilizar la infraestructura de Fibre Channel existente actualizada para admitir NVMe.

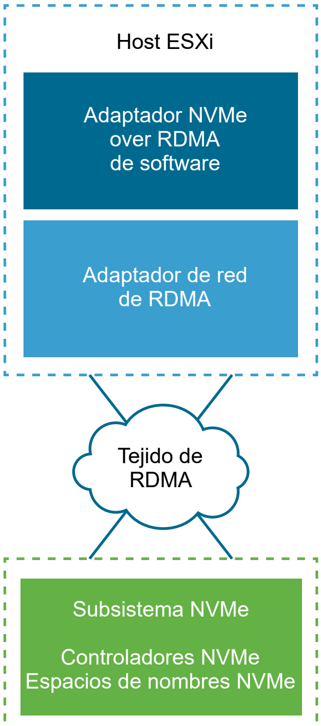
Para acceder al almacenamiento de NVMe over Fibre Channel, instale un adaptador de almacenamiento de Fibre Channel que admita NVMe en el host ESXi. No es necesario que configure el adaptador. Se conecta automáticamente a un subsistema de NVMe adecuado y detecta todos los dispositivos de almacenamiento de NVMe compartidos a los que puede acceder. Posteriormente, puede volver a configurar el adaptador y desconectar sus controladores o conectar otros controladores que no estaban disponibles durante el arranque del host. Para obtener más información, consulte Agregar controlador para NVMe over Fabrics.



NVMe over RDMA (RoCE V2)

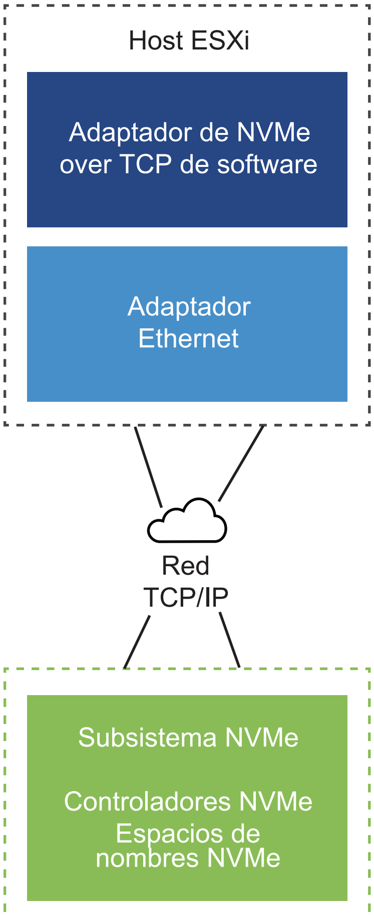
Esta tecnología utiliza un transporte de acceso de memoria directo remoto (Remote Direct Memory Access, RDMA) entre dos sistemas de la red. El transporte permite el intercambio de datos en la memoria principal omitiendo el sistema operativo o el procesador de cualquiera de los sistemas. ESXi admite la tecnología RDMA over Converged Ethernet V2 (RoCE V2), que habilita el acceso directo a la memoria remota a través de una red Ethernet.

Para acceder al almacenamiento, el host ESXi utiliza un adaptador de red de RDMA instalado en el host y un adaptador de almacenamiento de NVMe over RDMA de software. Debe configurar ambos adaptadores para usarlos para la detección de almacenamiento. Para obtener más información, consulte Configurar adaptadores para el almacenamiento de NVMe over RDMA (RoCE V2).



NVMe over TCP

Esta tecnología utiliza conexiones Ethernet entre dos sistemas. Para acceder al almacenamiento, el host ESXi utiliza un adaptador de red instalado en el host y un adaptador de almacenamiento de NVMe over TCP de software. Debe configurar ambos adaptadores para usarlos para la detección de almacenamiento. Para obtener más información, consulte Configurar adaptadores para almacenamiento de NVMe over TCP.



Requisitos y limitaciones del almacenamiento de NVMe de VMware

Cuando utilice la tecnología NVMe con VMware, siga las directrices y los requisitos específicos.

Requisitos para NVMe over PCIe

El entorno de almacenamiento de ESXi debe incluir los siguientes componentes:

- Dispositivos de almacenamiento de NVMe locales.
- Host compatible con ESXi.
- Adaptador de NVMe over PCIe de hardware. Después de instalar el adaptador, el host de ESXi lo detecta y se muestra en vSphere Client como adaptador de almacenamiento (vmhba) con el protocolo indicado como PCIe. No es necesario que configure el adaptador.

Requisitos para NVMe over RDMA (RoCE V2)

- Matriz de almacenamiento NVMe con compatibilidad con el transporte NVMe over RDMA (RoCE V2).

- Host compatible con ESXi.
- Conmutadores Ethernet que admiten una red sin pérdida.
- Adaptador de red compatible con RDMA over Converged Ethernet (RoCE v2). Para configurar el adaptador, consulte Ver adaptadores de red de RDMA.
- Adaptador NVMe over RDMA de software. Este componente de software debe estar habilitado en el host ESXi y conectado a un adaptador RDMA de red adecuado. Para obtener información, consulte Habilitar adaptadores de software de NVMe over RDMA o NVMe over TCP.
- Controlador de NVMe. Debe agregar un controlador después de configurar un adaptador NVMe over RDMA de software. Consulte Agregar controlador para NVMe over Fabrics.

Requisitos para NVMe over Fibre Channel

- Matriz de almacenamiento de Fibre Channel que admita NVMe. Para obtener información, consulte Capítulo 4 Usar ESXi con SAN de canal de fibra.
- Host compatible con ESXi.
- Adaptador NVMe de hardware. Por lo general, es un HBA de Fibre Channel que admite NVMe. Cuando se instala el adaptador, el host ESXi lo detecta, y se muestra en vSphere Client como un adaptador de Fibre Channel estándar (vmhba) con el protocolo de almacenamiento indicado como NVMe. No es necesario que configure el adaptador de NVMe de hardware para usarlo.
- Controlador de NVMe. No es necesario que configure el controlador. Después de instalar el adaptador NVMe de hardware necesario, se conecta automáticamente a todos los destinos y controladores a los que se puede acceder en ese momento. Posteriormente, puede desconectar los controladores o conectar otros controladores que no estaban disponibles durante el arranque del host. Consulte Agregar controlador para NVMe over Fabrics.

Requisitos para NVMe over TCP

- Matriz de almacenamiento NVMe con compatibilidad con el transporte NVMe over TCP.
- Host compatible con ESXi.
- Un adaptador Ethernet.
- Adaptador de NVMe over TCP de software. Este componente de software debe estar habilitado en el host ESXi y conectado a un adaptador de red adecuado. Para obtener más información, consulte Habilitar adaptadores de software de NVMe over RDMA o NVMe over TCP.
- Controlador de NVMe. Debe agregar un controlador después de configurar un adaptador NVMe over TCP de software. Consulte Agregar controlador para NVMe over Fabrics.

Compatibilidad con almacenamiento compartido de VMware NVMe over Fabrics

En el entorno de ESXi, los dispositivos de almacenamiento NVMe son similares a los dispositivos de almacenamiento SCSI y se pueden usar como almacenamiento compartido. Siga estas reglas cuando use el almacenamiento de NVMe-oF.

- No mezcle tipos de transporte para acceder al mismo espacio de nombres.
- Asegúrese de que las rutas activas se presenten al host. Los espacios de nombres no se pueden registrar hasta que se detecte la ruta de acceso activa.

Funcionalidad de almacenamiento compartido	Almacenamiento de SCSI over Fabric	Almacenamiento de NVMe over Fabric
RDM	Compatible	No compatible
Volcado de núcleo	Compatible	No compatible
Reservas de SCSI-2	Compatible	No compatible
VMDK agrupado en clúster	Compatible	No compatible
VMDK compartido con marca de multiescritura	Compatible	Compatible En vSphere 7.0 Update 1 y versiones posteriores. Para obtener más información, consulte el artículo de la base de conocimientos.
Virtual Volumes	Compatible	No compatible
Aceleración de hardware con complementos de VAAI	Compatible	No compatible
MPP predeterminado	NMP	HPP (NMP no puede reclamar los destinos NVMe-oF)
Límites	LUN = 1024, rutas de acceso = 4096	Espacios de nombres = 32, rutas de acceso = 128 (máximo 4 rutas de acceso por espacio de nombres en un host)

Configurar Ethernet sin pérdida para NVMe over RDMA

NVMe over RDMA en ESXi necesita una red Ethernet sin pérdida para poder funcionar de forma eficaz.

Para establecer redes sin pérdida, puede seleccionar una de las opciones de configuración de calidad de servicio disponibles.

Habilitar el control de flujo de pausa global

En esta configuración de red, asegúrese de que el control de flujo de pausa global esté habilitado en los puertos de conmutador de red. Compruebe también que las NIC compatibles con RDMA del host negocien automáticamente el control de flujo correcto.

Para comprobar el control de flujo, ejecute los siguientes comandos.

```
#esxcli network nic get -n vmnicX
   Pause RX: true
   Pause TX: true
```

Si las opciones de comando anteriores no se establecen en true, ejecute el siguiente comando.

```
#esxcli network nic pauseParams set -r true -t true -n vmnicX
```

Habilitar el control de flujo basado en prioridad (PFC, Priority Flow Control)

Para que el tráfico RoCE no tenga pérdidas, debe configurar el valor de prioridad de PFC en 3 en el conmutador físico y los hosts. El PFC se puede configurar en el host ESXi de dos maneras:

- Configuración automática. A partir de ESXi 7.0, la configuración de PFC de DCB se aplica automáticamente en la RNIC del host si el controlador de RNIC es compatible con DCB y DCBx.

  Para comprobar la configuración actual de DCB, ejecute el siguiente comando.

  ```
  #esxcli network nic dcb status get -n vmnicX
  ```

- Configuración manual. En algunos casos, los controladores de RNIC proporcionan un método para configurar manualmente el PFC de DCB mediante parámetros específicos de los controladores. Para utilizar este método, consulte la documentación del controlador específico del proveedor. Por ejemplo, en el controlador ConnectX-4/5 de Mellanox, puede establecer el valor de prioridad de PFC en 3 si ejecuta el siguiente comando y reinicia el host.

  ```
  #esxcli system module parameters set -m nmlx5_core -p "pfctx=0x08 pfcrx=0x08"
  ```

Habilitar PFC basado en DSCP

El PFC basado en DSCP es otra forma de configurar la red sin pérdida. En los hosts y los conmutadores físicos, debe establecer el valor de DSCP en 26. Para usar esta opción, consulte la documentación del controlador específico del proveedor. Por ejemplo, en el controlador ConnectX-4/5 de Mellanox, puede establecer el valor de etiqueta de DSCP en 26 si ejecuta los siguientes comandos.

- Habilitar el modo de confianza de PFC y DSCP

  ```
  #esxcli system module parameters set -m nmlx5_core -p "pfctx=0x08 pfcrx=0x08 trust_state=2"
  ```

- Establecer el valor de DSCP en 26

  ```
  #esxcli system module parameters set -m nmlx5_rdma -p "dscp_force=26"
  ```

- Verifique los parámetros que desea comprobar para confirmar si la configuración es correcta y si está establecida.

  ```
  esxcli system module parameters list -m nmlx5_core | grep 'trust_state\|pfcrx\|pfctx'
  ```

- Reiniciar el host

Configurar adaptadores para el almacenamiento de NVMe over RDMA (RoCE V2)

El proceso de configuración del adaptador del host ESXi implica la configuración del enlace de VMkernel para un adaptador de red de RDMA y, a continuación, la habilitación de un adaptador de NVMe over RDMA de software.

El siguiente vídeo le guiará por los pasos necesarios para configurar adaptadores NVMe over RDMA.

(Configurar adaptadores de NVMe over RDMA)

Procedimiento

1 Ver adaptadores de red de RDMA

  Después de instalar un adaptador de red que sea compatible con RDMA (RoCE V2) en el host ESXi, utilice vSphere Client para revisar el adaptador de RDMA y un adaptador de red físico.

2 Configurar el enlace de VMkernel para el adaptador de RDMA

  El enlace de puertos para NVMe over RDMA implica la creación de un conmutador y la conexión del adaptador de red físico y el adaptador de VMkernel al conmutador. A través de esta conexión, el adaptador de RDMA se enlaza al adaptador de VMkernel. En la configuración, puede usar un conmutador estándar de vSphere o un conmutador de vSphere Distributed Switch.

Pasos siguientes

Después de habilitar el adaptador de NVMe over RDMA de software, agregue controladores de NVMe para que el host pueda detectar los destinos de NVMe. Consulte Agregar controlador para NVMe over Fabrics.

Ver adaptadores de red de RDMA

Después de instalar un adaptador de red que sea compatible con RDMA (RoCE V2) en el host ESXi, utilice vSphere Client para revisar el adaptador de RDMA y un adaptador de red físico.

Procedimiento

1 En el host ESXi, instale un adaptador que admita RDMA (RoCE V2), por ejemplo, la familia MT27700 de Mellanox Technologies ConnectX-4.

   El host detecta el adaptador, y vSphere Client muestra sus dos componentes, un adaptador de RDMA y un adaptador de red físico.

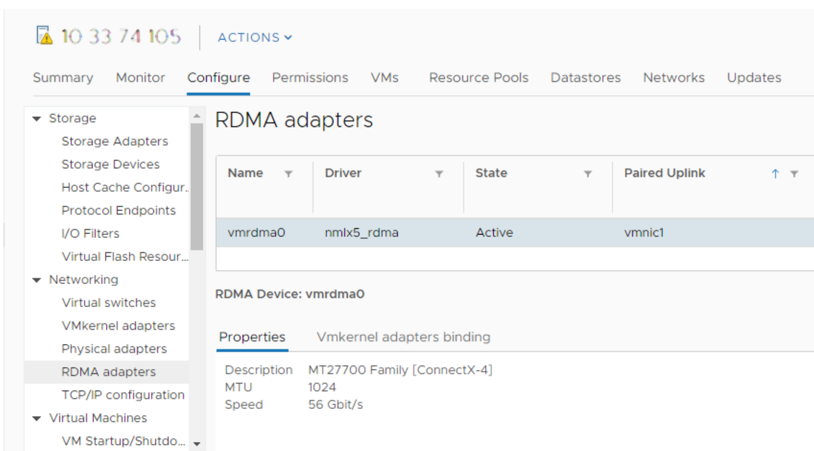
2 En vSphere Client, compruebe que el host detecte el adaptador de RDMA.

   a Desplácese hasta el host.

   b Haga clic en la pestaña **Configurar**.

   c En **Redes**, haga clic en **Adaptadores RDMA**.

   En este ejemplo, el adaptador RDMA aparece en la lista como `vmrdma0`. La columna **Vínculo superior emparejado** muestra el componente de red como el adaptador de red físico `vmnic1`.



   d Para comprobar la descripción del adaptador, seleccione el adaptador RDMA de la lista y haga clic en la pestaña **Propiedades**.

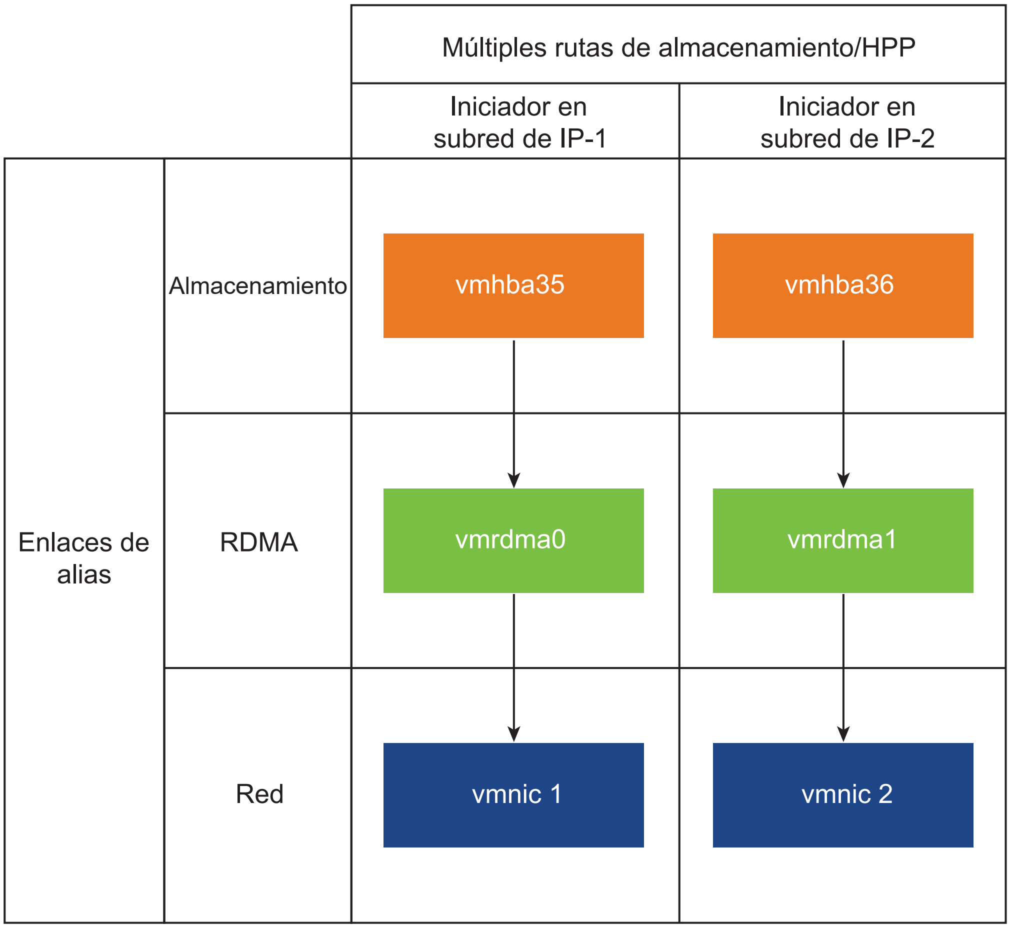
Pasos siguientes

Ahora puede crear el adaptador de NVMe over RDMA de software.

Configurar el enlace de VMkernel para el adaptador de RDMA

El enlace de puertos para NVMe over RDMA implica la creación de un conmutador y la conexión del adaptador de red físico y el adaptador de VMkernel al conmutador. A través de esta conexión, el adaptador de RDMA se enlaza al adaptador de VMkernel. En la configuración, puede usar un conmutador estándar de vSphere o un conmutador de vSphere Distributed Switch.

El siguiente diagrama muestra el enlace de puertos para el adaptador de NVMe over RDMA.

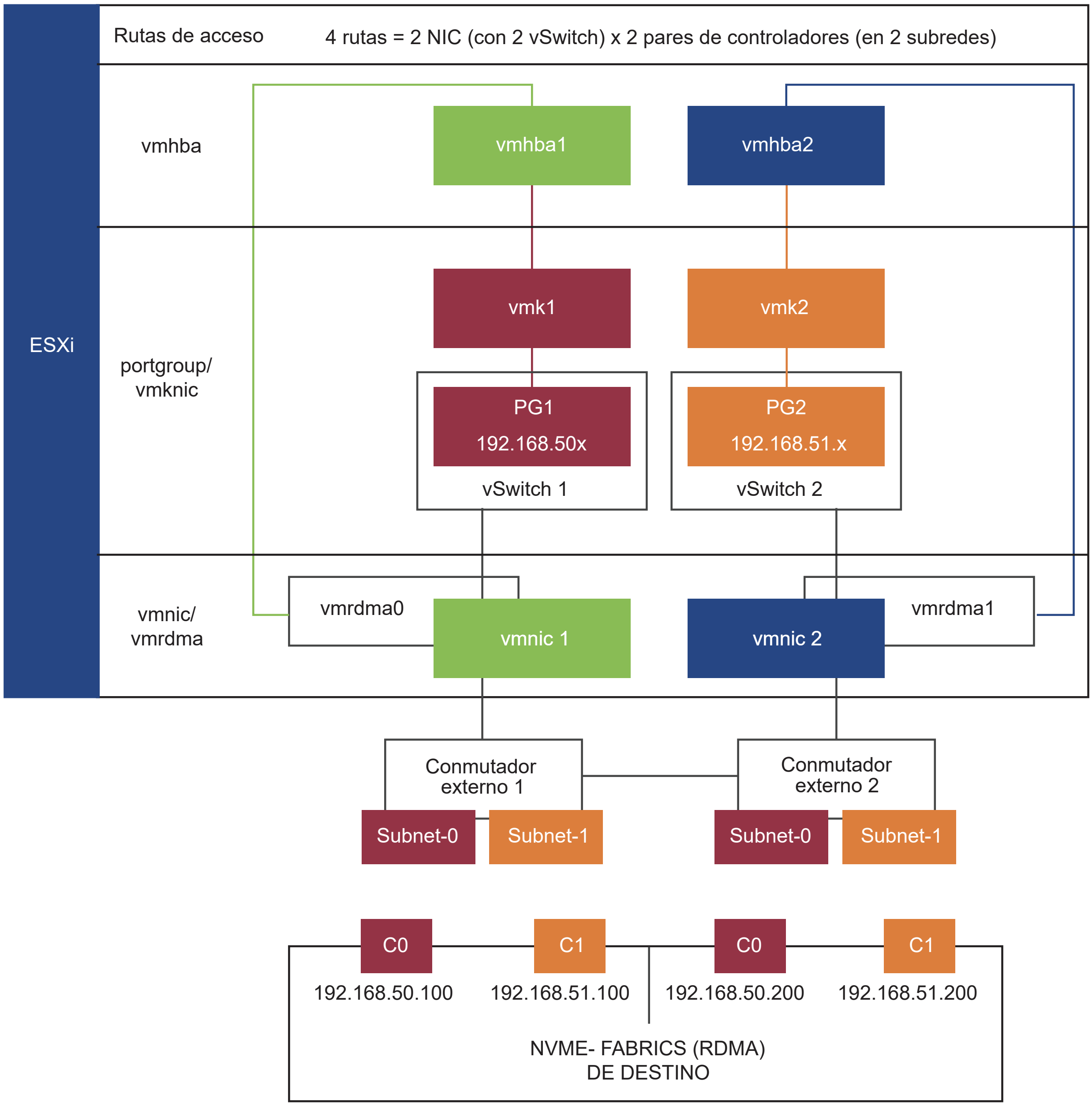


Para obtener información sobre la creación de conmutadores, consulte *Crear un conmutador estándar de vSphere* o *Crear vSphere Distributed Switch* en la documentación de *Redes de vSphere*.

Ejemplo de topología de red con NVMe over RDMA

En este ejemplo, dos conmutadores estándar de vSphere y dos vínculos superiores (NIC compatibles con RDMA) proporcionan una alta disponibilidad. Estos se conectan a dos pares de controladores en dos subredes.

HA con varios vSwitches y varios vínculos superiores (RNIC)



Configurar el enlace de VMkernel con un conmutador estándar de vSphere

El enlace de puertos de VMkernel se puede configurar para el adaptador de RDMA mediante un conmutador estándar de vSphere y un vínculo superior por conmutador. La configuración de la conexión de red implica la creación de un adaptador VMkernel virtual para cada adaptador de red físico. Use una asignación 1:1 entre cada adaptador de red física y virtual.

Procedimiento

1 Cree un conmutador estándar de vSphere con un adaptador de VMkernel y el componente de red.

a En vSphere Client, seleccione el host y haga clic en la pestaña **Redes**.

b Haga clic en **Acciones > Agregar redes**.

c Seleccione **Adaptador de red de VMkernel** y haga clic en **SIGUIENTE**.

d Seleccione **Nuevo conmutador estándar** y haga clic en **SIGUIENTE**.

e En **Adaptadores asignados**, haga clic en **+**.

Se mostrará la lista de adaptadores físicos disponibles.

f Seleccione el `vmnic` del adaptador físico que se requiere y haga clic en **Aceptar**.

Nota Asegúrese de seleccionar el adaptador de red físico que corresponda al adaptador de RDMA. Para ver la asociación entre el adaptador de RDMA `vmrdma` y el adaptador de red físico `vmnic`, consulte Ver adaptadores de red de RDMA.

---

g En **Configuración de puerto de VMkernel**, introduzca los valores necesarios.

Si utiliza una VLAN para la ruta de almacenamiento, introduzca el ID de VLAN.

h En la lista **Configuración de IP**, introduzca la configuración de IPv4 de VMkernel.

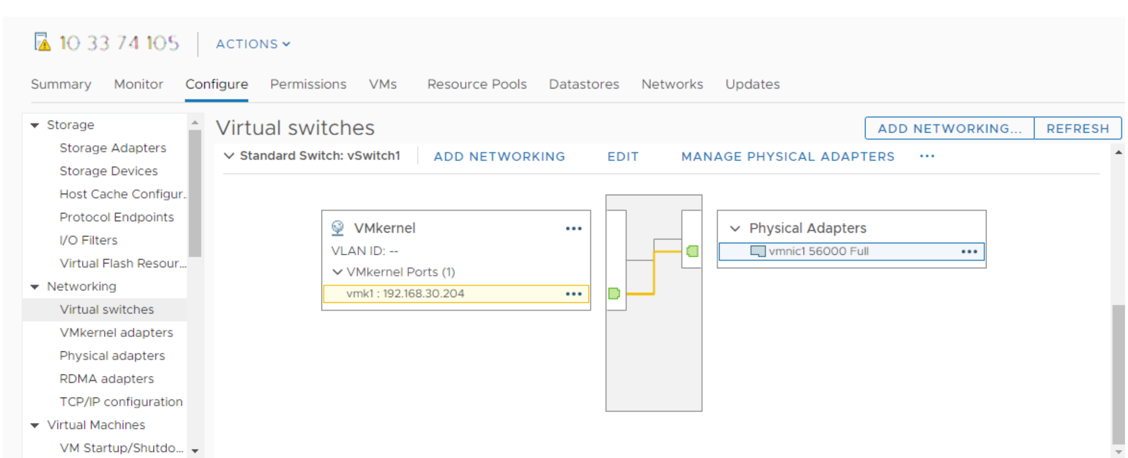
i En Servicios disponibles, seleccione **NVMe over RDMA**.

2 Compruebe que el conmutador esté configurado correctamente.

a En la pestaña **Configurar**, seleccione **Conmutadores virtuales** en **Redes**.

b Expanda el conmutador y compruebe su configuración.

La ilustración muestra que el adaptador de red físico y el adaptador de VMkernel están conectados al conmutador estándar de vSphere. A través de esta conexión, el adaptador de RDMA se enlaza al adaptador de VMkernel.

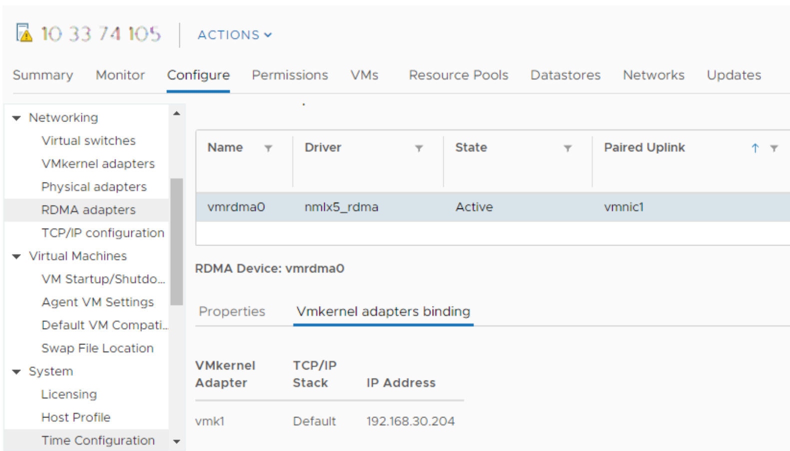


3 Compruebe la configuración del enlace de VMkernel para el adaptador de RDMA.

   a En la lista **Redes**, haga clic en **Adaptadores RDMA** y seleccione el adaptador de RDMA en la lista.

   b Haga clic en la pestaña **Enlace de adaptadores de VMkernel** y compruebe que el adaptador de VMkernel asociado aparezca en la página.

   En este ejemplo, el adaptador de RDMA `vmrdma0` está emparejado con el adaptador de red `vmnic1` y está conectado al adaptador de VMkernel `vmk1`.



Configurar el enlace de VMkernel con un conmutador estándar de vSphere y la formación de equipos de NIC

El enlace de puertos de VMkernel se puede configurar para el adaptador de RDMA mediante un conmutador estándar de vSphere con la configuración de la formación de equipos de NIC. Puede utilizar la formación de equipos de NIC para lograr la redundancia de red. Puede configurar dos o más adaptadores de red (NIC) como un equipo para obtener un alto nivel de disponibilidad y equilibrio de carga.

Procedimiento

1 Cree un conmutador estándar de vSphere con un adaptador de VMkernel y el componente de red con la configuración de la formación de equipos de NIC.

   a En vSphere Client, seleccione el host y haga clic en la pestaña **Redes**.

   b Haga clic en **Acciones > Agregar redes**.

   c Seleccione **Adaptador de red de VMkernel** y haga clic en **SIGUIENTE**.

   d Seleccione **Nuevo conmutador estándar** y haga clic en **SIGUIENTE**.

   e En **Adaptadores asignados**, haga clic en **+**.

   Aparece una lista de los adaptadores físicos disponibles.

   f Seleccione el `vmnic` del adaptador físico que se requiere y agréguelo en **Adaptadores activos**.

g Seleccione otro `vmnic` de adaptador físico y agréguelo en **Adaptadores sin utilizar**.

h En **Configuración de puerto de VMkernel**, introduzca los valores necesarios.

Si utiliza una VLAN para la ruta de almacenamiento, introduzca el ID de VLAN.

i En la lista **Configuración de IP**, especifique la configuración de IPv4 de VMkernel.

j En Servicios disponibles, seleccione **NVMe over RDMA**.

Repita el paso 1 para configurar un conmutador estándar existente.

2 Configure su conmutador para la configuración de formación de equipos de NIC .

a Haga clic en la pestaña **Configurar** y seleccione **Conmutadores virtuales** en **Redes**.

b Seleccione el adaptador de VMkernel adecuado.

c En el menú contextual, haga clic en **Editar configuración**.

d Seleccione **Formación de equipos y conmutación por error**.

e En **Adaptadores activos**, mueva el `vmnic` de adaptador físico que se requiere.

f En **Adaptadores en espera > Orden de conmutación por error**, mueva los otros adaptadores físicos.

g Establezca el equilibrio de carga adecuado y otras propiedades.

h Repita los pasos para configurar algunos adaptadores de VMkernel adicionales.

3 Repita los pasos 1 y 2 para agregar y configurar un conjunto adicional de instancias de `rnic` de equipo. Para comprobar si el adaptador está configurado, haga clic en la pestaña **Configurar** y seleccione **Adaptadores de VMkernel**.

Configurar el enlace de VMkernel con vSphere Distributed Switch

El enlace de puertos de VMkernel se puede configurar para el adaptador de RDMA mediante una instancia de vSphere Distributed Switch y un vínculo superior por conmutador. La configuración de la conexión de red implica la creación de un adaptador VMkernel virtual para cada adaptador de red físico. Use una asignación 1:1 entre cada adaptador de red física y virtual.

Procedimiento

1 Cree una instancia de vSphere Distributed Switch con un adaptador de VMkernel y el componente de red.

a En vSphere Client, seleccione **Centro de datos** y haga clic en la pestaña **Redes**.

b Haga clic en **Acciones** y seleccione **Distributed Switch > Nuevo Distributed Switch**.

c Seleccione un nombre para el conmutador.

Compruebe que la ubicación del centro de datos esté presente en el host y haga clic en **Siguiente**.

d Seleccione la versión de ESXi como **7.0.0 y versiones posteriores** y, a continuación, haga clic en **Siguiente**.

e Introduzca la cantidad de vínculos superiores que se pide y haga clic en **Finalizar**.

2 Agregue uno o varios hosts al conmutador virtual distribuido.

a En vSphere Client, seleccione **Centro de datos** y haga clic en **Conmutadores distribuidos**.

Aparece entonces una lista de conmutadores distribuidos disponibles.

b Haga clic con el botón derecho en el conmutador distribuido y seleccione **Agregar y administrar hosts** en el menú.

c Seleccione **Agregar hosts** y haga clic en **Siguiente**.

d Seleccione el host y haga clic en **Siguiente**.

e Seleccione **Asignar vínculo superior**.

f Introduzca el vínculo superior relevante para asignar `vmnic`.

g Asigne un adaptador de VMkernel y haga clic en **Siguiente**.

h En vSphere Client, seleccione el conmutador distribuido y haga clic en la pestaña **Puertos**.

Aquí podrá ver los vínculos superiores que se han creado para el conmutador.

3 Cree grupos de puertos distribuidos para la ruta de almacenamiento de NVMe over RDMA.

a En vSphere Client, seleccione el conmutador distribuido que se pide.

b Haga clic en **Acciones** y seleccione **Grupo de puertos distribuidos > Nuevo grupo de puertos distribuidos**.

c En **Configurar parámetros**, introduzca las propiedades generales del grupo de puertos.

Si configuró una VLAN específica, agréguela en el ID de VLAN.

Nota Si no configura la VLAN correctamente, pueden surgir problemas de conectividad de red.

---

4 Configure los adaptadores de VMkernel.

a En vSphere Client, expanda la lista **DSwitch** y seleccione el grupo de puertos distribuidos.

b Haga clic en **Acciones > Agregar adaptadores de VMkernel**.

c En el cuadro de diálogo **Seleccionar hosts miembro**, seleccione el host y haga clic en **Aceptar**.

d En el cuadro de diálogo **Configurar adaptador de VMkernel**, asegúrese de que la MTU coincida con la MTU del conmutador.

e En **Servicios disponibles**, seleccione **NVMe over RDMA** para un etiquetado adecuado.

f Haga clic en **Finalizar**.

g Repita los pasos b y c para agregar varias NIC compatibles con RDMA.

5 Establezca las directivas de formación de equipos de NIC para los grupos de puertos distribuidos.

   a En **Grupo de puertos distribuidos**, haga clic en **Acciones > Editar configuración**.

   b Haga clic en **Formación de equipos y conmutación por error** y compruebe los vínculos superiores activos.

   c Asigne un vínculo superior como **Activo** para el grupo de puertos y el otro vínculo superior como **Sin utilizar**.

   Repita el paso c para cada uno de los grupos de puertos creados.

Pasos siguientes

Después de completar la configuración, haga clic en **Configurar** y compruebe si la pestaña del adaptador físico del host muestra el DVSwitch de las NIC seleccionadas.

Configurar adaptadores para almacenamiento de NVMe over TCP

El proceso de configuración del adaptador del host ESXi implica la configuración del enlace de VMkernel para un adaptador de red de TCP y, a continuación, la habilitación de un adaptador de NVMe over TCP de software.

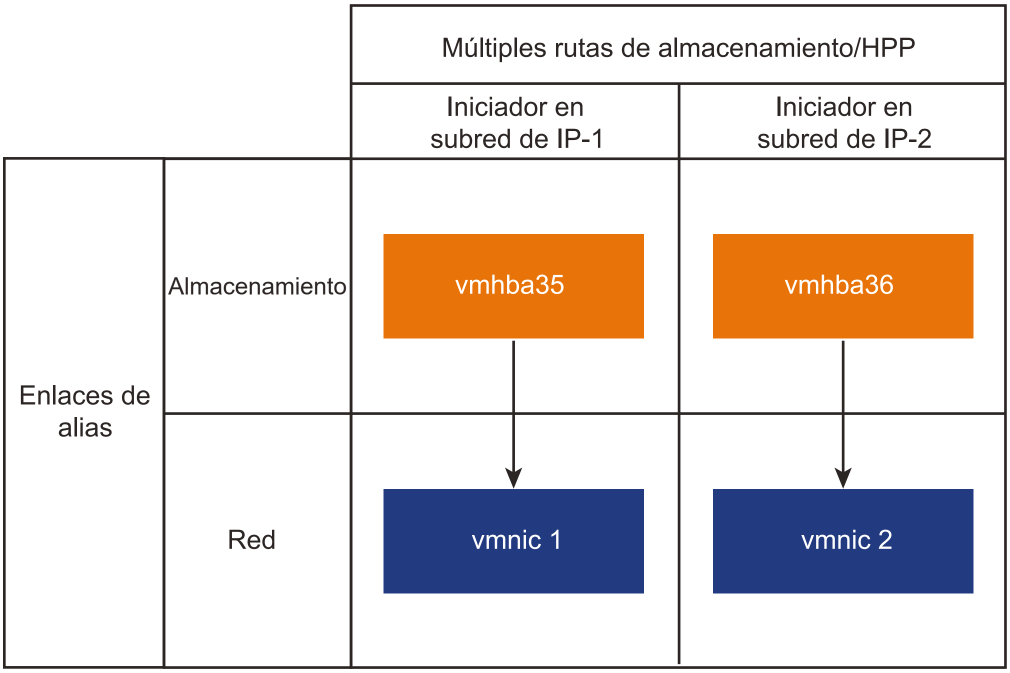
Pasos siguientes

Después de habilitar el adaptador de NVMe over TCP de software, agregue controladoras NVMe para que el host pueda detectar los destinos de NVMe. Para obtener más información, consulte Agregar controlador para NVMe over Fabrics.

Configurar el enlace de VMkernel para el adaptador de NVMe over TCP

El enlace de puertos para NVMe over TCP implica la creación de un conmutador virtual y la conexión del adaptador de red físico y el adaptador de VMkernel al conmutador virtual. A través de esta conexión, el adaptador TCP se enlaza al adaptador de VMkernel. En la configuración, puede usar un conmutador estándar de vSphere o un conmutador de vSphere Distributed Switch.

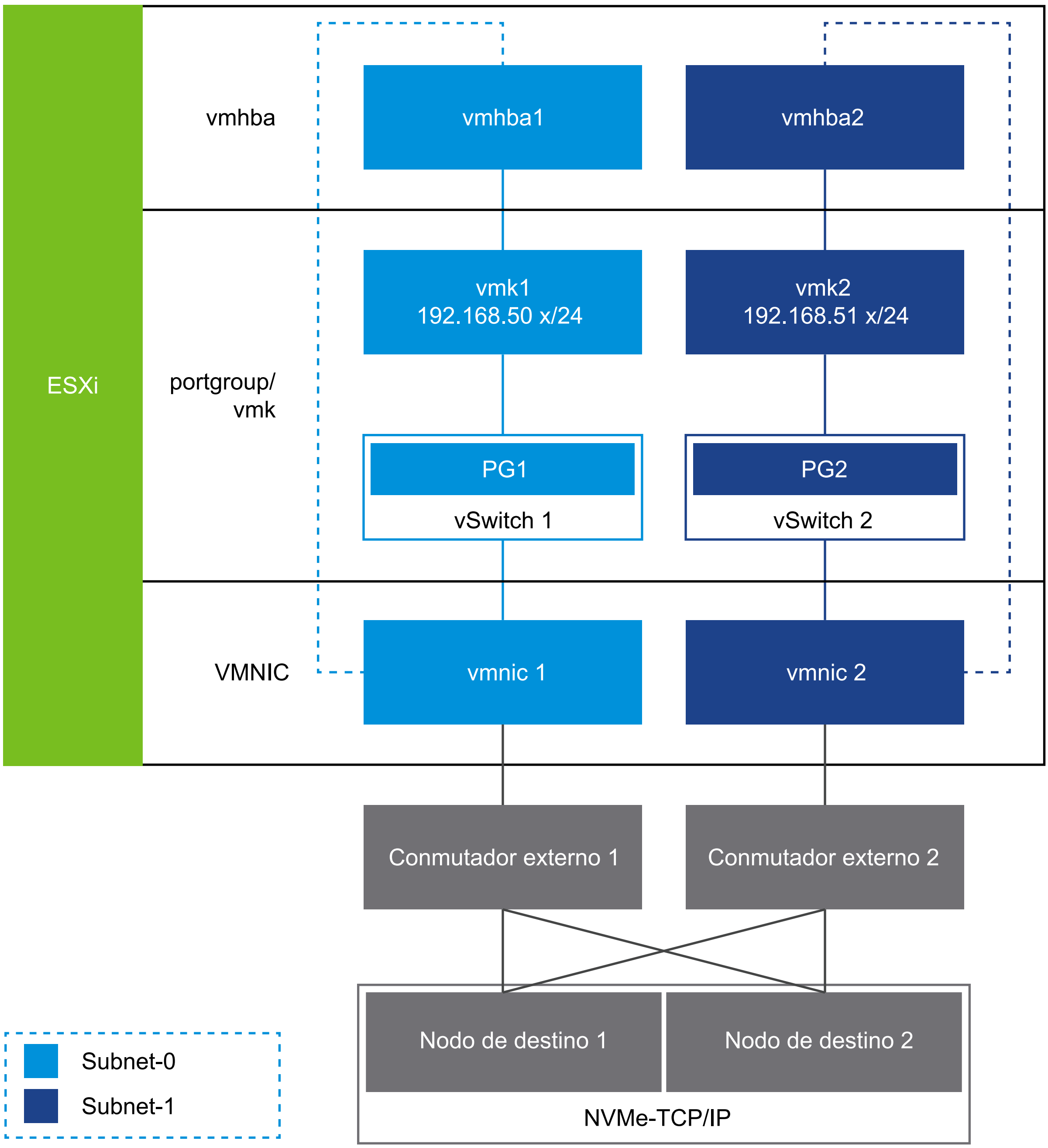
El siguiente diagrama muestra el enlace de puertos para el adaptador de NVMe over TCP.



Para obtener información sobre la creación de conmutadores, consulte *Crear un conmutador estándar de vSphere* o *Crear vSphere Distributed Switch* en la documentación de *Redes de vSphere*.

Ejemplo de topología de red con NVMe over TCP

En este ejemplo, dos conmutadores estándar de vSphere y dos adaptadores de red (vmnic) en el host proporcionan alta disponibilidad. Se conectan a dos conmutadores externos.



Configurar el enlace de VMkernel para el adaptador TCP con un conmutador estándar de vSphere

El enlace de puerto de VMkernel se puede configurar para el adaptador de TCP mediante un conmutador estándar de vSphere y un vínculo superior por conmutador. La configuración de la conexión de red implica la creación de un adaptador VMkernel virtual para cada adaptador de red físico. Use una asignación 1:1 entre cada adaptador de red física y virtual.

Procedimiento

1 Cree un conmutador estándar de vSphere con un adaptador de VMkernel y el componente de red.

a En vSphere Client, seleccione el host y haga clic en la pestaña **Redes**.

b Haga clic en **Acciones > Agregar redes**.

c Seleccione **Adaptador de red de VMkernel** y haga clic en **SIGUIENTE**.

d Seleccione **Nuevo conmutador estándar** y haga clic en **SIGUIENTE**.

e En **Adaptadores asignados**, haga clic en **+**.

Se mostrará la lista de adaptadores físicos disponibles.

f Seleccione el `vmnic` del adaptador físico que se requiere y haga clic en **Aceptar**.

Nota Asegúrese de seleccionar el adaptador de red físico que corresponda al adaptador TCP/IP.

g En **Configuración de puerto de VMkernel**, introduzca los valores necesarios.

Si utiliza una VLAN para la ruta de almacenamiento, introduzca el ID de VLAN.

h En la lista **Configuración de IP**, introduzca la configuración de IPv4 de VMkernel.

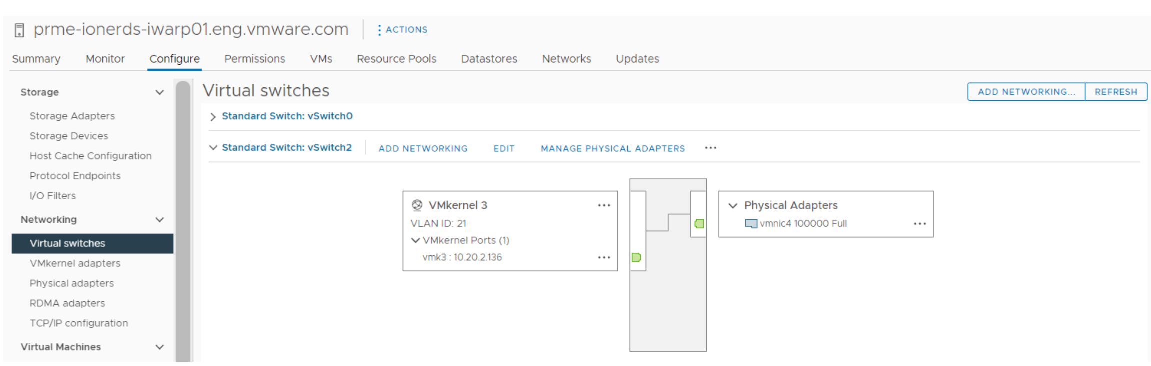
i En **Servicios disponibles**, seleccione **NVMe over TCP** para el etiquetado adecuado.

2 Compruebe que el conmutador esté configurado correctamente.

a En la pestaña **Configurar**, seleccione **Conmutadores virtuales** en **Redes**.

b Expanda el conmutador y compruebe su configuración.

La ilustración muestra que el adaptador de red físico y el adaptador de VMkernel están conectados al conmutador estándar de vSphere. A través de esta conexión, el adaptador TCP se enlaza al adaptador de VMkernel.



3 Establezca directivas de formación de equipos de NIC para el conmutador estándar de vSphere.

Nota El adaptador NVMe/TCP no admite funciones de formación de equipos de NIC como la conmutación por error y el equilibrio de carga. En su lugar, se basa en storage multipathing para estas funcionalidades. Sin embargo, si debe configurar la formación de equipos de NIC para otras cargas de trabajo de red en el vínculo superior que presta servicio al adaptador NVMe/TCP, siga estos pasos.

a Haga clic en la pestaña **Configurar** y seleccione **Conmutadores virtuales** en **Redes**.

b Seleccione el adaptador de VMkernel adecuado.

c En el menú contextual, haga clic en **Editar configuración**.

d Seleccione **Formación de equipos y conmutación por error**.

e En **Adaptadores activos**, mueva el `vmnic` de adaptador físico que se requiere.

f En **Adaptadores en espera > Orden de conmutación por error**, mueva los otros adaptadores físicos.

g Establezca el equilibrio de carga adecuado y otras propiedades.

h Repita los pasos para configurar algunos adaptadores de VMkernel adicionales.

Para comprobar si el adaptador está configurado, haga clic en la pestaña **Configurar** y seleccione **Adaptadores de VMkernel**.

Configurar el enlace de VMkernel para el adaptador de TCP con un conmutador distribuido de vSphere

El enlace de puerto de VMkernel se puede configurar para el adaptador de TCP mediante una instancia de vSphere Distributed Switch y un vínculo superior por conmutador. La configuración de la conexión de red implica la creación de un adaptador VMkernel virtual para cada adaptador de red físico. Use una asignación 1:1 entre cada adaptador de red física y virtual.

Procedimiento

1 Cree una instancia de vSphere Distributed Switch con un adaptador de VMkernel y el componente de red.

a En vSphere Client, seleccione **Centro de datos** y haga clic en la pestaña **Redes**.

b Haga clic en **Acciones** y seleccione **Distributed Switch > Nuevo Distributed Switch**.

c Seleccione un nombre para el conmutador.

Compruebe que la ubicación del centro de datos esté presente en el host y haga clic en **Siguiente**.

d Seleccione la versión de ESXi como **ESXi 7.0 y versiones posteriores** y, a continuación, haga clic en **Siguiente**.

e Introduzca la cantidad de vínculos superiores que se pide y haga clic en **Finalizar**.

2 Agregue uno o varios hosts al conmutador virtual distribuido.

   a En vSphere Client, seleccione **Centro de datos** y haga clic en **Conmutadores distribuidos**.

      Aparece entonces una lista de conmutadores distribuidos disponibles.

   b Haga clic con el botón derecho en el conmutador distribuido y seleccione **Agregar y administrar hosts** en el menú.

   c Seleccione **Agregar hosts** y haga clic en **Siguiente**.

   d Seleccione el host y haga clic en **Siguiente**.

   e Seleccione **Asignar vínculo superior**.

   f Introduzca el vínculo superior relevante para asignar `vmnic`.

   g Asigne un adaptador de VMkernel y haga clic en **Siguiente**.

   h En vSphere Client, seleccione el conmutador distribuido y haga clic en la pestaña **Puertos**.

      Aquí podrá ver los vínculos superiores que se han creado para el conmutador.

3 Cree grupos de puertos distribuidos para la ruta de almacenamiento de NVMe over TCP.

   a En vSphere Client, seleccione el conmutador distribuido que se pide.

   b Haga clic en **Acciones** y seleccione **Grupo de puertos distribuidos > Nuevo grupo de puertos distribuidos**.

   c En **Configurar parámetros**, introduzca las propiedades generales del grupo de puertos.

      Si configuró una VLAN específica, agréguela en el ID de VLAN.

      Nota Si no configura la VLAN correctamente, pueden surgir problemas de conectividad de red.

4 Configure los adaptadores de VMkernel.

   a En vSphere Client, expanda la lista **DSwitch** y seleccione el grupo de puertos distribuidos.

   b Haga clic en **Acciones > Agregar adaptadores de VMkernel**.

   c En el cuadro de diálogo **Seleccionar hosts miembro**, seleccione el host y haga clic en **Aceptar**.

   d En el cuadro de diálogo **Configurar adaptador de VMkernel**, asegúrese de que la MTU coincida con la MTU del conmutador.

   e Haga clic en **Finalizar**.

   f Repita los pasos b y c para agregar varias NIC compatibles con TCP.

5 Establezca las directivas de formación de equipos de NIC para los grupos de puertos distribuidos.

Nota El adaptador NVMe/TCP no admite funciones de formación de equipos de NIC como la conmutación por error y el equilibrio de carga. En su lugar, se basa en storage multipathing para estas funcionalidades. Sin embargo, si debe configurar la formación de equipos de NIC para otras cargas de trabajo de red en el vínculo superior que presta servicio al adaptador NVMe/TCP, siga estos pasos.

a En **Grupo de puertos distribuidos**, haga clic en **Acciones > Editar configuración**.

b Haga clic en **Formación de equipos y conmutación por error** y compruebe los vínculos superiores activos.

c Asigne un vínculo superior como **Activo** para el grupo de puertos y el otro vínculo superior como **Sin utilizar**.

Repita el paso c para cada uno de los grupos de puertos creados.

Pasos siguientes

Después de completar la configuración, haga clic en **Configurar** y compruebe si la pestaña del adaptador físico del host muestra el DVSwitch de las NIC seleccionadas.

Habilitar adaptadores de software de NVMe over RDMA o NVMe over TCP

ESXi admite adaptadores de software NVMe over RDMA y NVMe over TCP. Utilice vSphere Client para habilitar los adaptadores de almacenamiento de software para NVMe over RDMA y NVMe over TCP.

Requisitos previos

- En el host ESXi, instale un adaptador que admita los siguientes tipos de almacenamiento.
  - Adaptador NVMe over RDMA. Por ejemplo, Mellanox Technologies MT27700 Family ConnectX-4.
  - Adaptador NVMe over TCP. Por ejemplo, i40en.
- Configure el enlace de VMkernel para los adaptadores.
  - Para NVMe over RDMA, consulte Configurar el enlace de VMkernel para el adaptador de RDMA.
  - Para NVMe over TCP, consulte Configurar el enlace de VMkernel para el adaptador de NVMe over TCP.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y, a continuación, en el icono **Agregar adaptador de software**.

4 Seleccione el tipo de adaptador según sea necesario.

   - **Adaptador NVMe over RDMA**
   - **Adaptador NVMe over TCP**

5 Según la selección que realice en el paso 4, seleccione un adaptador RDMA adecuado o un adaptador de red TCP (`vmnic`) en el menú desplegable.

   Nota Si aparece un mensaje de error que le impide crear el adaptador de software, asegúrese de que esté configurado correctamente el enlace de VMkernel para el adaptador. Para obtener más información, consulte Configurar el enlace de VMkernel para el adaptador de RDMA y Configurar el enlace de VMkernel para el adaptador de NVMe over TCP.

Resultados

Los adaptadores de software de NVMe over RDMA y NVMe over TCP aparecen en la lista como adaptadores de almacenamiento de `vmhba`. Puede quitar los adaptadores si necesita liberar el adaptador de red de RDMA y TCP subyacente para otros fines.

Agregar controlador para NVMe over Fabrics

Utilice vSphere Client para agregar un controlador de NVMe. Después de agregar el controlador, los espacios de nombres de NVMe asociados con este pasan a estar disponibles para el host ESXi. Los dispositivos de almacenamiento de NVMe que representan los espacios de nombres en el entorno de ESXi aparecen en la lista de dispositivos de almacenamiento.

Si utiliza el almacenamiento de NVMe over RDMA (RoCE V2), debe agregar un controlador después de configurar un adaptador de NVMe over RDMA de software. Si utiliza el almacenamiento de NVMe over TCP, debe agregar un controlador después de configurar un adaptador de NVMe over TCP de software. Con el almacenamiento de FC-NVMe, después de instalar el adaptador necesario, se conecta automáticamente a todos los destinos a los que se puede acceder en ese momento. Posteriormente, puede volver a configurar el adaptador y desconectar sus controladores o conectar otros controladores que no estaban disponibles durante el arranque del host.

Requisitos previos

Asegúrese de que el host ESXi tenga los adaptadores adecuados para su tipo de almacenamiento. Consulte Requisitos y limitaciones del almacenamiento de NVMe de VMware.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione el adaptador (vmhba#) que desea configurar.

4 Haga clic en la pestaña **Controladores** y, a continuación, en **Agregar controlador**.

5 Para agregar el controlador, seleccione una de las siguientes opciones y haga clic en **Agregar**.

Opción	Descripción
Detectar automáticamente controladoras	Este método indica que el host puede aceptar una conexión a cualquier controlador disponible. a Especifique el siguiente parámetro para un controlador de detección. ■ Para NVMe over RDMA (RoCE V2), la dirección IP y el número de puerto de transporte. ■ Para NVMe over TCP, la dirección IP, el número de puerto de transporte y el parámetro de resumen. b Haga clic en **Detectar controladores**. c En la lista de controladores, seleccione el controlador que desea utilizar.
Introduzca manualmente los detalles del controlador.	Con este método, el host solicita una conexión a un controlador específico con los siguientes parámetros: ■ NQN de subsistema ■ Identificación de puerto de destino. Para NVMe over RDMA (RoCE V2), la dirección IP y el número de puerto de transporte (opcional). Para FC-NVMe, WorldWideNodeName y WorldWidePortName. ■ Para NVMe over TCP, la dirección IP, el número de puerto de transporte (opcional) y el parámetro de resumen (opcional). ■ Tamaño de cola de administración. Un parámetro opcional que especifica el tamaño de la cola de administración del controlador. El valor predeterminado es 16. ■ Tiempo de espera de conexión persistente. Un parámetro opcional para especificar en segundos el tiempo de espera de conexión persistente entre el adaptador y el controlador. El valor predeterminado es 60 segundos. ■ Tamaño de cola de E/S y número de cola de E/S. Parámetros opcionales que solo se pueden establecer a través de esxcli.

Resultados

El controlador aparece en la lista de controladores. Ahora el host puede detectar los espacios de nombres de NVMe que están asociados al controlador. Los dispositivos de almacenamiento de NVMe que representan los espacios de nombres en el entorno de ESXi aparecen en la lista de dispositivos de almacenamiento de vSphere Client.

Eliminar adaptadores de software de NVMe over RDMA y TCP

Utilice el vSphere Client para eliminar adaptadores de software NVMe over RDMA y TCP. Puede quitar el adaptador si necesita liberar el adaptador de red de RDMA subyacente o el adaptador ethernet para otros fines.

No se pueden eliminar los adaptadores de NVMe over PCIe y FC-NVMe.

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione el adaptador (`vmhba#`) que desea quitar.
4. Elimine el controlador de NVMe conectado al adaptador.
   a. Haga clic en la pestaña **Controladores**.
   b. Seleccione el controlador y haga clic en **Eliminar**.

      El controlador de NVMe se desconecta y desaparece de la lista.
5. Haga clic en el icono **Eliminar** (eliminar el adaptador de almacenamiento del host) para eliminar el adaptador de NVMe over RDMA el adaptador de NVMe over TCP.

Trabajar con almacenes de datos

17

Los almacenes de datos son contenedores lógicos, de manera análoga a los sistemas de archivos, que ocultan aspectos específicos de almacenamiento físico y ofrecen un modelo uniforme para almacenar archivos de máquinas virtuales. Los almacenes de datos también pueden utilizarse para almacenar imágenes ISO, plantillas de máquinas virtuales e imágenes de disquete.

Este capítulo incluye los siguientes temas:

Tipos de almacenes de datos

Según el almacenamiento que se utilice, los almacenes de datos pueden ser de diferentes tipos.

vCenter Server y ESXi admiten los siguientes tipos de almacenes de datos.

Tabla 17-1. Tipos de almacenes de datos

Tipo de almacén de datos	Descripción
VMFS (versión 5 y 6)	Los almacenes de datos que se implementan en dispositivos de almacenamiento de bloques usan el formato vSphere Virtual Machine File System (VMFS). VMFS es un formato de sistema de archivos de alto rendimiento optimizado para el almacenamiento de máquinas virtuales. Consulte Descripción de los almacenes de datos de VMFS.
NFS (versión 3 y 4.1)	Un cliente NFS integrado en ESXi utiliza el protocolo Network File System (NFS) mediante TCP/IP para acceder a un volumen NFS designado. El volumen se encuentra en un servidor NAS. El host ESXi monta el volumen como almacén de datos NFS y lo utiliza para el almacenamiento. ESXi es compatible con las versiones 3 y 4.1 del protocolo NFS. Consulte Describir los almacenes de datos de Network File System
vSAN	vSAN agrega todos los dispositivos de capacidad local disponibles en los hosts a un solo almacén de datos compartido por todos los hosts del clúster de vSAN. Consulte la documentación de *Administrar VMware vSAN*.
vVol	El almacén de datos de Virtual Volumes representa un contenedor de almacenamiento en vCenter Server y en vSphere Client. Consulte Capítulo 22 Trabajar con VMware vSphere Virtual Volumes.

Según el tipo de almacenamiento, algunas de las siguientes tareas están disponibles para los almacenes de datos.

- Cree almacenes de datos. Puede utilizar vSphere Client para crear ciertos tipos de almacenes de datos.
- Realice operaciones administrativas en los almacenes de datos. Varias operaciones, como el cambio de nombre de un almacén de datos, están disponibles para todos los tipos de almacenes de datos. Otras aplican a tipos de almacenes de datos específicos.
- Organice los almacenes de datos. Por ejemplo, agrupándolos en carpetas de acuerdo con las prácticas de negocios. Después de agrupar los almacenes de datos, se pueden asignar los mismos permisos y alarmas a los almacenes de datos del grupo al mismo tiempo.
- Agregue los almacenes de datos a los clústeres de almacenes de datos. Un clúster de almacenes de datos es una colección de almacenes de datos con recursos compartidos y una interfaz de administración compartida. Cuando crea un clúster de almacén de datos, se puede usar Storage DRS para administrar recursos de almacenamiento. Para obtener información sobre los clústeres de almacenes de datos, consulte la documentación de *Administrar recursos de vSphere*.

Descripción de los almacenes de datos de VMFS

Para almacenar discos virtuales, ESXi usa almacenes de datos. Los almacenes de datos son contenedores lógicos que ocultan los detalles específicos del almacenamiento físico ante las máquinas virtuales y proporcionan un modelo uniforme para el almacenamiento de archivos de máquina virtual. Los almacenes de datos que se implementan en dispositivos de almacenamiento de bloques usan el formato nativo de vSphere Virtual Machine File System (VMFS). Se trata de un formato de sistema de archivos de alto rendimiento optimizado para el almacenamiento de máquinas virtuales.

Utilice vSphere Client para configurar un almacén de datos de VMFS con anticipación en un dispositivo de almacenamiento en bloque que el host ESXi pueda detectar. El almacén de datos de VMFS puede extenderse para abarcar varios dispositivos de almacenamiento físico, incluidos LUN de SAN y almacenamiento local. Esta característica permite agrupar almacenamiento y brinda flexibilidad para crear el almacén de datos necesario para las máquinas virtuales.

Puede incrementar la capacidad de un almacén de datos mientras las máquinas virtuales se están ejecutando en el almacén de datos. Esta capacidad permite agregar espacio nuevo a los almacenes de datos de VMFS a medida que la máquina virtual lo requiera. VMFS está diseñado para el acceso simultáneo desde varias máquinas físicas y aplica los controles de acceso adecuados a los archivos de máquinas virtuales.

Versiones de almacenes de datos de VMFS

Se han publicado varias versiones del sistema de archivos VMFS desde su creación. Actualmente, ESXi admite VMFS5 y VMFS6.

Para todas las versiones de VMFS admitidas, ESXi ofrece compatibilidad completa de lectura y escritura. En los almacenes de datos de VMFS compatibles, puede crear y encender máquinas virtuales.

Tabla 17-2. Acceso del host a las versiones de VMFS

VMFS	ESXi
VMFS 6	Lectura y escritura
VMFS5	Lectura y escritura

En la siguiente tabla, se comparan las principales características de VMFS5 y VMFS6. Para obtener información adicional, consulte *Máximos de configuración*.

Tabla 17-3. Comparación de VMFS5 y VMFS6

Funciones y funcionalidades	VMFS5	VMFS 6
Acceso para hosts ESXi 6.5 y versiones posteriores	Sí	Sí
Acceso para hosts ESXi 6.0 y versiones anteriores	Sí	No
Almacenes de datos por host	512	512

Tabla 17-3. Comparación de VMFS5 y VMFS6 (continuación)

Funciones y funcionalidades	VMFS5	VMFS 6
Dispositivos de almacenamiento 512n	Sí	Sí (valor predeterminado)
Dispositivos de almacenamiento 512e	Sí. No compatible en dispositivos 512e locales.	Sí (valor predeterminado)
Dispositivos de almacenamiento 4Kn	No	Sí
Recuperación de espacio automática	No	Sí
Recuperación de espacio manual mediante el comando esxcli. Consulte Recuperar manualmente espacio de almacenamiento acumulado.	Sí	Sí
Recuperación de espacio por parte del sistema operativo invitado	Limitada	Sí
Partición de dispositivo de almacenamiento GPT	Sí	Sí
Partición de dispositivo de almacenamiento MBR	Sí Para un almacén de datos de VMFS5 que se actualizó anteriormente desde VMFS3.	No
Dispositivos de almacenamiento de más de 2 TB para cada extensión de VMFS	Sí	Sí
Compatibilidad con máquinas virtuales con discos virtuales de gran capacidad o discos superiores a 2 TB	Sí	Sí
Compatibilidad con archivos pequeños de 1 KB	Sí	Sí
Uso predeterminado de mecanismos de bloqueo solo con ATS en dispositivos de almacenamiento compatibles con ATS. Consulte Mecanismos de bloqueo de VMFS.	Sí	Sí
Tamaño de bloque	1 MB estándar	1 MB estándar
Instantáneas predeterminadas	VMFSsparse para discos virtuales inferiores a 2 TB SEsparse para discos virtuales superiores a 2 TB	SEsparse
Tipo de emulación de disco virtual	512n	512n
vMotion	Sí	Sí
Storage vMotion en diferentes tipos de almacenes de datos	Sí	Sí
Alta disponibilidad y Fault Tolerance	Sí	Sí
DRS y Storage DRS	Sí	Sí
RDM	Sí	Sí

Cuando trabaje con almacenes de datos de VMFS, tenga en cuenta lo siguiente:

- Extensiones de almacenes de datos. Un almacén de datos de VMFS expandido solo debe usar dispositivos de almacenamiento homogéneos, ya sean 512n, 512e o 4Kn. El almacén de datos expandido no puede extenderse en dispositivos de diferentes formatos.
- Tamaño de bloque. El tamaño de bloque de un almacén de datos de VMFS define el tamaño de archivo máximo y la cantidad de espacio que ocupa un archivo. Los almacenes de datos de VMFS5 y VMFS6 admiten el tamaño de bloque de 1 MB.
- Storage vMotion. Storage vMotion admite la migración entre almacenes de datos de VMFS, vSAN y Virtual Volumes. vCenter Server realiza comprobaciones de compatibilidad para validar Storage vMotion entre diferentes tipos de almacén de datos.
- Storage DRS. VMFS5 y VMFS6 pueden coexistir en el mismo clúster de almacén de datos. Sin embargo, todos los almacenes de datos en el clúster deben usar dispositivos de almacenamiento homogéneos. No combine dispositivos de diferentes formatos dentro del mismo clúster de almacén de datos.
- Formatos de partición de dispositivos. Los almacenes de datos de VMFS5 o VMFS6 nuevos usan la tabla de partición GUID (GPT) para dar formato al dispositivo de almacenamiento. El formato de GPT permite crear almacenes de datos de más de 2 TB. Si el almacén de datos de VMFS5 ya se actualizó de la versión VMFS3, sigue usando el formato de partición de registro de arranque maestro (Master Boot Record, MBR) característico de VMFS3. La conversión a GPT se produce solo después de expandir el almacén de datos a un tamaño mayor que 2 TB.

Almacenes de datos de VMFS como repositorios

ESXi puede dar formato a los dispositivos de almacenamiento basados en SCSI como almacenes de datos de VMFS. Los almacenes de datos de VMFS actúan principalmente como repositorios de máquinas virtuales.

Nota Asimismo, siempre se debe tener un solo almacén de datos de VMFS para cada LUN.

Es posible almacenar varias máquinas virtuales en el mismo almacén de datos de VMFS. Cada máquina virtual, encapsulada en un conjunto de archivos, ocupa un único directorio separado. En el sistema operativo dentro de la máquina virtual, VMFS preserva la semántica del sistema de archivos interno, que garantiza el comportamiento correcto de la aplicación y la integridad de los datos de las aplicaciones que se ejecutan en las máquinas virtuales.

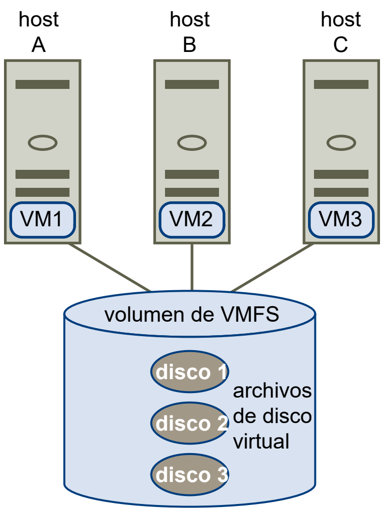
Cuando se ejecutan varias máquinas virtuales, VMFS proporciona mecanismos de bloqueo específicos para los archivos de máquina virtual. En consecuencia, las máquinas virtuales pueden operar sin problemas en un entorno de SAN en el que varios hosts ESXi comparten un mismo almacén de datos de VMFS.

Además de las máquinas virtuales, los almacenes de datos de VMFS pueden almacenar otros archivos, como plantillas de máquina virtual e imágenes ISO.

Compartir un almacén de datos de VMFS entre hosts

Como sistema de archivos de clúster, VMFS permite que varios hosts ESXi accedan a los mismos almacenes de datos de VMFS de manera simultánea.

Figura 17-1. Compartir un almacén de datos de VMFS entre hosts



Para obtener información sobre la cantidad máxima de hosts que pueden conectarse a un solo almacén de datos de VMFS, consulte el documento de *Valores máximos de configuración*.

Para impedir que varios hosts accedan a la misma máquina virtual a la vez, VMFS ofrece bloqueo en disco.

Compartir el volumen VMFS entre varios hosts ofrece varias ventajas, por ejemplo:

- Se pueden utilizar VMware Distributed Resource Scheduling (DRS) y VMware High Availability (HA).

  Se pueden distribuir máquinas virtuales en diferentes servidores físicos. Esto significa que se ejecuta una combinación de máquinas virtuales en cada servidor para que no todos experimenten una demanda alta en la misma área al mismo tiempo. Si un servidor genera un error, es posible reiniciar las máquinas virtuales en otro servidor físico. Si hay un error, se activa el bloqueo en disco de cada máquina virtual. Para obtener más información sobre VMware DRS, consulte la documentación de *Administrar recursos de vSphere*. Para obtener información sobre VMware HA, consulte la documentación de *Disponibilidad de vSphere*.

- vMotion se puede utilizar para migrar máquinas virtuales en ejecución de un servidor físico al otro. Para obtener información sobre la migración de máquinas virtuales, consulte la documentación de *Administrar vCenter Server y hosts*.

Para crear un almacén de datos compartido, móntelo en los hosts ESXi que requieran acceso al almacén de datos. Consulte Montar almacenes de datos.

Actualizaciones de metadatos de VMFS

Un almacén de datos de VMFS incluye archivos, directorios, enlaces simbólicos, archivos de descriptores RDM, etc. de máquinas virtuales. El almacén de datos también mantiene una vista coherente de toda la información de asignación de estos objetos. Esta información de asignación se denomina metadatos.

Los metadatos se actualizan cada vez que se realizan operaciones de administración de almacenes de datos o máquinas virtuales. Algunos ejemplos de operaciones que requieren actualizaciones de metadatos son los siguientes:

- Creación, ampliación o bloqueo de un archivo de máquina virtual
- Cambio de atributos de un archivo
- Encendido o apagado de una máquina virtual
- Creación o eliminación de un almacén de datos de VMFS
- Expansión de un almacén de datos de VMFS
- Creación de una plantilla
- Implementación de una máquina virtual desde una plantilla
- Migración de una máquina virtual con vMotion

Cuando los cambios en los metadatos se realizan en un entorno de almacenamiento compartido, VMFS utiliza mecanismos de bloqueo especiales para proteger sus datos y evitar que varios hosts escriban en los metadatos de manera simultánea.

Mecanismos de bloqueo de VMFS

En un entorno de almacenamiento compartido, cuando varios hosts acceden al mismo almacén de datos de VMFS, se utilizan mecanismos de bloqueo específicos. Estos mecanismos de bloqueo evitan que varios hosts escriban simultáneamente en los metadatos y garantiza que no se dañen los datos.

Según la configuración y el tipo de almacenamiento subyacente, un almacén de datos de VMFS puede utilizar diferentes tipos de mecanismos de bloqueo. Puede utilizar exclusivamente el mecanismo de bloqueo de prueba y configuración atómica (solo ATS), o bien usar una combinación de ATS y reservas SCSI (ATS+SCSI).

Mecanismo de solo ATS

En el caso de los dispositivos de almacenamiento que admiten especificaciones de VAAI basadas en estándares T10, VMFS proporciona bloqueo de ATS, también denominado bloqueo asistido por hardware. El algoritmo de ATS admite el bloqueo discreto por sector de disco. Todos los almacenes de datos de VMFS5 y VMFS6 con formato nuevo usan el mecanismo de solo ATS si el almacenamiento subyacente lo admite, y nunca usan reservas SCSI.

Cuando crea un almacén de datos multiextensión que usa ATS, vCenter Server filtra los dispositivos que no son ATS. Este filtrado permite usar solo aquellos dispositivos que admiten ATS primitiva.

En ciertos casos, es posible que deba para cambiar el mecanismo de bloqueo predeterminado para un almacén de datos de VMFS5 o VMFS6. Para obtener información, consulte Cambiar el mecanismo de bloqueo a ATS+SCSI.

Nota Si ejecuta un entorno de VMware vSAN o tiene volúmenes VMFS solo con ATS, no desactive ATS. Desactivar ATS puede provocar una interrupción debido a que no hay ningún mecanismo de bloqueo disponible. Para obtener más información, consulte un artículo de la base de conocimientos de VMware.

Mecanismo ATS+SCSI

Un almacén de datos de VMFS que admite el mecanismo ATS+SCSI está configurado para usar ATS e intenta usarlo cuando es posible. Si ATS presenta errores, el almacén de datos de VMFS se revierte a las reservas SCSI. A diferencia del bloqueo de ATS, las reservas SCSI bloquean un dispositivo de almacenamiento completo mientras se realiza una operación que requiere protección de metadatos. Una vez completada la operación, VMFS libera la reserva y las otras operaciones pueden continuar.

Los almacenes de datos que usan el mecanismo ATS+SCSI incluyen almacenes de datos VMFS5 que se actualizaron desde VMFS3. Además, los almacenes de datos de VMFS5 o VMFS6 nuevos en dispositivos de almacenamiento que no admiten ATS usan el mecanismo ATS+SCSI.

Si el almacén de datos de VMFS se revierte a las reservas de SCSI, es posible que note una degradación en el rendimiento provocada por reservas de SCSI excesivas.

Mostrar información de bloqueo de VMFS

Utilice el comando `esxcli` para obtener información sobre el mecanismo de bloqueo que utiliza un almacén de datos de VMFS.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

- Para mostrar información relacionada con mecanismos de bloqueo de VMFS, ejecute el siguiente comando:

  ```
  esxcli storage vmfs lockmode list
  ```

Resultados

La tabla enumera elementos que podría incluir la salida del comando.

Tabla 17-4. Información de bloqueo de VMFS

Campos	Valores	Descripciones
Modos de bloqueo		Indica la configuración de bloqueo del almacén de datos.
	`ATS`	El almacén de datos está configurado para usar el modo de bloqueo solo con ATS.
	`ATS+SCSI`	El almacén de datos está configurado para usar el modo de bloqueo ATS. Si ATS falla o no es compatible, el almacén de datos puede revertir a SCSI.
	`ATS upgrade pending`	El almacén de datos está en el proceso de una actualización en línea al modo de bloqueo solo con ATS.
	`ATS downgrade pending`	El almacén de datos está en el proceso de una degradación en línea al modo de bloqueo ATS+SCSI.
Compatible con ATS		Indica si el almacén de datos puede estar configurado o no para el modo de bloqueo solo con ATS.
Modos de actualización de ATS		Indica el tipo de actualización compatible con el almacén de datos.
	`None`	El almacén de datos no es compatible con el mecanismo de bloqueo solo con ATS.
	`Online`	El almacén de datos puede utilizarse durante su actualización al modo de bloqueo solo con ATS.
	`Offline`	El almacén de datos no puede utilizarse durante su actualización al modo de bloqueo solo con ATS.
Motivo de incompatibilidad con ATS		Si el almacén de datos no es compatible con el mecanismo de bloqueo solo con ATS, el elemento indica el motivo de la incompatibilidad.

Cambiar bloqueo de VMFS al modo de solo con ATS

Si el almacén de datos de VMFS utiliza el mecanismo de bloqueo ATS+SCSI, puede cambiarlo al modo de bloqueo solo con ATS.

Por lo general, los almacenes de datos de VMFS5 que se actualizaron de VMFS3 siguen utilizando el mecanismo de bloqueo ATS+SCSI. Si los almacenes de datos se implementan en hardware compatible con ATS, cumplen los requisitos para actualizarse al modo de bloqueo solo con ATS. Según el entorno de vSphere, se puede utilizar uno de los siguientes modos de actualización:

- La actualización en línea del mecanismo solo con ATS está disponible para la mayoría de los almacenes de datos VMFS5 de una sola extensión. Mientras se realiza la actualización en línea en uno de los hosts, otros hosts pueden seguir utilizando el almacén de datos.
- La actualización sin conexión a bloqueo solo con ATS debe utilizarse en almacenes de datos VMFS5 que abarcan varias extensiones físicas. Los almacenes de datos compuestos por varias extensiones no cumplen los requisitos para la actualización en línea. Estos almacenes de datos requieren que ningún host utilice activamente los almacenes de datos en el momento de la solicitud de actualización.

Procedimiento

1 Preparación de una actualización a bloqueo solo con ATS

   Debe seguir varios pasos para preparar el entorno para una actualización en línea o sin conexión al bloqueo solo con ATS.

2 Actualización del mecanismo de bloqueo al tipo solo con ATS

   Si un almacén de datos de VMFS es compatible solo con ATS, es posible actualizar su mecanismo de bloqueo de ATS+SCSI a solo con ATS.

Preparación de una actualización a bloqueo solo con ATS

Debe seguir varios pasos para preparar el entorno para una actualización en línea o sin conexión al bloqueo solo con ATS.

Procedimiento

1 Actualice todos los hosts que acceden al almacén de datos VMFS5 a la versión más nueva de vSphere.

2 Para determinar si el almacén de datos cumple con los requisitos para una actualización de su mecanismo de bloqueo actual, ejecute el comando `esxcli storage vmfs lockmode list`.

   La siguiente salida de ejemplo indica que el almacén de datos es apto para una actualización. También muestra el mecanismo de bloqueo actual y el modo de actualización disponible para el almacén de datos.

```
Locking Mode  ATS Compatible  ATS Upgrade Modes
------------  --------------  -----------------
ATS+SCSI           true       Online or Offline
```

3 Según el modo de actualización disponible para el almacén de datos, realice una de las siguientes acciones:

Modo de actualización	Acción
En línea	Compruebe que todos los hosts tengan una conectividad de almacenamiento coherente con el almacén de datos de VMFS.
Sin conexión	Compruebe que ningún host esté utilizando activamente el almacén de datos.

Actualización del mecanismo de bloqueo al tipo solo con ATS

Si un almacén de datos de VMFS es compatible solo con ATS, es posible actualizar su mecanismo de bloqueo de ATS+SCSI a solo con ATS.

La mayoría de los almacenes de datos que no expanden varias extensiones cumplen con los requisitos de una actualización en línea. Mientras se realiza la actualización en línea en uno de los hosts ESXi, otros hosts pueden seguir utilizando el almacén de datos. La actualización en línea se completa solo después de que todos los hosts hayan cerrado el almacén de datos.

Requisitos previos

Si planea completar la actualización del mecanismo de bloqueo colocando el almacén de datos en modo de mantenimiento, deshabilite Storage DRS. Este requisito previo se aplica solo a una actualización en línea.

Procedimiento

1 Para realizar una actualización del mecanismo de bloqueo, ejecute el siguiente comando:

   `esxcli storage vmfs lockmode set -a|--ats -l|--volume-label=` *etiqueta de VMFS* `-u|--volume-uuid=` *VMFS UUID*.

2 Para una actualización en línea, se requieren pasos adicionales.

   a Cierre el almacén de datos en todos los hosts que tengan acceso al almacén de datos, de modo que los hosts puedan reconocer el cambio.

      Puede utilizar uno de los siguientes métodos:

      - Desmontar y montar el almacén de datos.
      - Colocar el almacén de datos en modo de mantenimiento y salir del modo de mantenimiento.

   b Compruebe que el estado de Modo de bloqueo del almacén de datos haya cambiado a Solo con ATS. Para hacerlo, ejecute el comando siguiente:

      ```
      esxcli storage vmfs lockmode list
      ```

   c Si el modo de bloqueo muestra cualquier otro estado (por ejemplo, Actualización de ATS pendiente), compruebe qué host aún no procesó la actualización. Para ello, ejecute el comando siguiente:

      ```
      esxcli storage vmfs host list
      ```

Cambiar el mecanismo de bloqueo a ATS+SCSI

Al crear un almacén de datos VMFS5 en un dispositivo que admite el bloqueo de prueba y configuración atómica (Atomic test and set, ATS), el almacén de datos usa el mecanismo de bloqueo solo con ATS. En ciertas circunstancias, es posible que deba degradar el bloqueo solo con ATS a ATS+SCSI.

Es posible que deba cambiar al mecanismo de bloqueo ATS+SCSI si, por ejemplo, se degrada el dispositivo de almacenamiento o si se produce un error en las actualizaciones de firmware y el dispositivo ya no es compatible con ATS.

El proceso de degradación es similar a la actualización solo a ATS. Al igual que con la actualización, según la configuración de almacenamiento, podrá realizar la degradación en modo en línea o sin conexión.

Nota Si ejecuta un entorno de VMware vSAN o tiene volúmenes VMFS solo con ATS, no desactive ATS. Desactivar ATS puede provocar una interrupción debido a que no hay ningún mecanismo de bloqueo disponible. Para obtener más información, consulte un artículo de la base de conocimientos de VMware.

Procedimiento

1 Para cambiar el mecanismo de bloqueo a ATS+SCSI, ejecute el siguiente comando:

   `esxcli storage vmfs lockmode set -s|--scsi -l|--volume-label=` *etiqueta de VMFS* `-u|--volume-uuid=` *VMFS UUID*.

2 Para el modo en línea, cierre el almacén de datos en todos los hosts que tengan acceso al almacén de datos, de modo que los hosts puedan reconocer el cambio.

Formatos de instantánea en VMFS

Cuando se crea una instantánea, se conserva el estado del disco virtual, lo que impide que el sistema operativo invitado escriba datos en él. Además, se crea un disco delta o secundario. El disco delta representa la diferencia entre el estado actual del disco de la máquina virtual y el estado que tenía en el momento en que se creó la instantánea anterior. En el almacén de datos de VMFS, el disco delta es un disco disperso.

Los discos dispersos usan el mecanismo de copia en escritura, en el cual el disco virtual no contiene datos hasta que se copian allí mediante una operación de escritura. Esta optimización ahorra espacio de almacenamiento.

Según el tipo de almacén de datos, los discos delta usan diferentes formatos dispersos.

Formatos de instantáneas	VMFS5	VMFS 6
VMFSsparse	Para discos virtuales inferiores a 2 TB.	N/C
SEsparse	Para discos virtuales superiores a 2 TB.	Para todos los discos.

VMFSsparse

VMFS5 usa el formato VMFSsparse para los discos virtuales de hasta 2 TB.

VMFSsparse se implementa sobre VMFS. La capa VMFSsparse procesa las E/S emitidas a una máquina virtual de instantánea. Técnicamente, VMFSsparse es un registro de rehacer que comienza vacío inmediatamente después de la creación de una instantánea de máquina virtual. El registro de rehacer se expande hasta alcanzar el tamaño de su vmdk base cuando se vuelve a escribir la vmdk con nuevos datos después de la creación de una instantánea de máquina virtual. El registro de rehacer es un archivo en el almacén de datos de VMFS. Tras la creación de una instantánea, la vmdk base asociada a la máquina virtual se transfiere a la vmdk dispersa recién creada.

SEsparse

SEsparse es un formato predeterminado para todos los discos delta en los almacenes de datos de VMFS6. En VMFS5, SEsparse se utiliza para discos virtuales de 2 TB o más.

SEsparse es un formato similar a VMFSsparse con algunas mejoras. Este formato ocupa menos espacio y es compatible con la técnica de recuperación de espacio. Con esta técnica, se marcan los bloques que elimina el SO invitado. El sistema envía comandos a la capa SEsparse del hipervisor para cancelar la asignación de esos bloques. Esta cancelación de asignación permite recuperar el espacio asignado por SEsparse una vez que el sistema operativo invitado eliminó los datos. Para obtener más información sobre la recuperación de espacio, consulte Recuperación de espacio de almacenamiento.

Migración de instantáneas

Se pueden migrar máquinas virtuales con instantáneas entre diferentes almacenes de datos. Se deben tener en cuenta las siguientes consideraciones:

- Si se migra una máquina virtual con una instantánea VMFSsparse a VMFS6, el formato de la instantánea cambia a SEsparse.
- Cuando se migra una máquina virtual con una vmdk de hasta 2 TB a VMFS5, el formato de la instantánea cambia a VMFSsparse.
- No se pueden mezclar los registros de rehacer VMFSsparse con los registros de rehacer SEsparse en la misma jerarquía.

Actualizar los almacenes de datos de VMFS

ESXi emplea diferentes enfoques para las actualizaciones de VMFS5 y VMFS3.

Almacenes de datos de VMFS5

No se puede actualizar un almacén de datos de VMFS5 a VMFS6. Si tiene un almacén de datos de VMFS5 en su entorno, cree un almacén de datos de VMFS6 y migre las máquinas virtuales del almacén de datos VMFS5 a VMFS6.

Almacenes de datos de VMFS3

ESXi ya no es compatible con almacenes de datos de VMFS3. El host ESXi actualiza automáticamente VMFS3 a VMFS5 al montar almacenes de datos existentes. El host realiza la operación de actualización en las siguientes circunstancias:

- En el primer arranque después de una actualización a ESXi 7.0 o una versión posterior, cuando el host monta todos los almacenes de datos de VMFS3 detectados.
- Cuando se montan manualmente los almacenes de datos de VMFS3 que se detectan después del arranque, o se montan de forma persistente los almacenes de datos desmontados.

Describir los almacenes de datos de Network File System

Un cliente NFS integrado en ESXi utiliza el protocolo Network File System (NFS) mediante TCP/IP para acceder a un volumen NFS designado ubicado en un servidor NAS. El host ESXi puede montar el volumen y utilizarlo para sus necesidades de almacenamiento. vSphere es compatible con las versiones 3 y 4.1 del protocolo NFS.

En general, un administrador de almacenamiento crea el directorio o el volumen NFS, y este se exporta del servidor NFS. No es necesario dar formato al volumen NFS con un sistema de archivos local, como VMFS. En cambio, se debe montar el volumen directamente en los hosts ESXi y utilizarlo para almacenar y arrancar máquinas virtuales del mismo modo en que se utilizan los almacenes de datos de VMFS.

Además de almacenar discos virtuales en almacenes de datos NFS, se puede utilizar NFS como un repositorio central de imágenes ISO, plantillas de máquina virtual, etc. Si utiliza el almacén de datos para las imágenes ISO, puede conectar el dispositivo de CD-ROM de la máquina virtual a un archivo ISO en el almacén de datos. Luego, puede instalar un sistema operativo invitado desde el archivo ISO.

Protocolos NFS y ESXi

ESXi es compatible con protocolos NFS versión 3 y 4.1. Para admitir ambas versiones, ESXi usa dos clientes NFS diferentes.

Comparación de versiones de clientes NFS

En la siguiente tabla, se enumeran las capacidades que admiten las versiones 3 y 4.1 de NFS.

Características	NFS versión 3	NFS versión 4.1
Mecanismos de seguridad	AUTH_SYS	AUTH_SYS y Kerberos (krb5 y krb5i)
Algoritmos de cifrado con Kerberos	N/C	AES256-CTS-HMAC-SHA1-96 y AES128-CTS-HMAC-SHA1-96
Múltiples rutas	No compatible	Compatible mediante el enlace troncal de sesiones
Mecanismos de bloqueo	Bloqueo de propiedad del lado del cliente	Bloqueo del lado del servidor

Características	NFS versión 3	NFS versión 4.1
Aceleración de hardware	Compatible	Compatible
Discos virtuales gruesos	Compatible	Compatible
IPv6	Compatible	Compatible con AUTH_SYS y Kerberos
Imágenes ISO presentadas como CD-ROM a las máquinas virtuales	Compatible	Compatible
Instantáneas de la máquina virtual	Compatible	Compatible
Máquinas virtuales con discos virtuales de más de 2 TB	Compatible	Compatible

Protocolos NFS y soluciones de vSphere

En la siguiente tabla, se enumeran las principales soluciones de vSphere que admiten las versiones de NFS.

Características de vSphere	NFS versión 3	NFS versión 4.1
vMotion y Storage vMotion	Sí	Sí
High Availability (HA)	Sí	Sí
Fault Tolerance (FT)	Sí	Sí
Distributed Resource Scheduler (DRS)	Sí	Sí
Perfiles de host	Sí	Sí
Storage DRS	Sí	No
Storage I/O Control	Sí	No
Site Recovery Manager	Sí	Site Recovery Manager no admite almacenes de datos NFS 4.1 para la replicación basada en matrices y la replicación de Virtual Volumes. Puede usar Site Recovery Manager con almacenes de datos NFS v 4.1 para vSphere Replication.
Virtual Volumes	Sí	Sí
vSphere Replication	Sí	Sí
vRealize Operations Manager	Sí	Sí

NFS 4.1 y Fault Tolerance

Las máquinas virtuales en NFS 4.1 admiten el nuevo mecanismo de tolerancia a errores incorporado en vSphere 6.0. El mecanismo puede alojar máquinas virtuales con multiprocesador simétrico (SMP) de hasta cuatro vCPU.

Las máquinas virtuales de NFS 4.1 no admiten el mecanismo heredado de la tolerancia a errores.

Actualizaciones de NFS

Cuando se actualiza ESXi desde una versión anterior a 6.5, los almacenes de datos NFS 4.1 existentes comienzan a admitir automáticamente las funcionalidades que no estaban disponibles en la versión anterior de ESXi. Estas funcionalidades incluyen Virtual Volumes, aceleración de hardware, etc.

ESXi no admite conversiones automáticas del almacén de datos de la versión 3 a la versión 4.1 de NFS.

Si desea actualizar un almacén de datos NFS 3, las siguientes opciones están disponibles:

- Crear el almacén de datos NFS 4.1 y luego utilizar Storage vMotion para migrar máquinas virtuales del almacén de datos anterior al nuevo.
- Utilizar los métodos de conversión que proporciona el servidor de almacenamiento NFS. Para obtener más información, póngase en contacto con su proveedor de almacenamiento.
- Desmontar el almacén de datos NFS 3 y montar el almacén de datos NFS 4.1.

  Precaución Si utiliza esta opción, asegúrese de desmontar el almacén de datos de todos los hosts que tengan acceso al almacén de datos. El almacén de datos jamás podrá montarse al utilizar ambos protocolos al mismo tiempo.

Instrucciones y requisitos de almacenamiento NFS

Al utilizar el almacenamiento NFS, siga las directrices específicas para la configuración del servidor NFS, las redes, los almacenes de datos NFS, etc.

- Configuración de servidores NFS

  Al configurar servidores NFS para trabajar con ESXi, siga las recomendaciones del proveedor de almacenamiento. Además de estas recomendaciones generales, siga las directrices específicas para NFS en un entorno vSphere.

- Redes en NFS

  Un host ESXi usa la conexión de red TCP/IP para acceder a un servidor NAS remoto. Existen algunas directrices y prácticas recomendadas para configurar las redes cuando se utiliza el almacenamiento NFS.

- Bloqueo de archivos NFS

  Los mecanismos de bloqueo de archivos permiten restringir el acceso a los datos almacenados en un servidor únicamente a un usuario o proceso por vez. Los mecanismos de bloqueo de las dos versiones de NFS no son compatibles. NFS 3 utiliza un bloqueo de propiedad y NFS 4.1 utiliza el bloqueo especificado del protocolo nativo.

- Seguridad de NFS

  Con NFS 3 y NFS 4.1, ESXi es compatible con el sistema de seguridad AUTH_SYS. Además, para NFS 4.1, también se admite el mecanismo de seguridad Kerberos.

- Uso de múltiples rutas en NFS

  NFS 4.1 admite múltiples rutas en función de las especificaciones del protocolo. Para NFS 3, no se pueden aplicar las múltiples rutas.

- NFS y aceleración de hardware

  Los discos virtuales creados en los almacenes de datos NFS reciben aprovisionamiento fino de forma predeterminada. Para poder crear discos virtuales con aprovisionamiento grueso, es necesario utilizar una aceleración de hardware que admita la operación de reserva de espacio.

- Almacenes de datos NFS

  Al crear un almacén de datos NFS, recuerde seguir las directrices específicas.

Configuración de servidores NFS

Al configurar servidores NFS para trabajar con ESXi, siga las recomendaciones del proveedor de almacenamiento. Además de estas recomendaciones generales, siga las directrices específicas para NFS en un entorno vSphere.

Las directrices incluyen los siguientes puntos.

- Asegúrese de que los servidores NAS que utiliza estén enumerados en *VMware HCL*. Utilice la versión correcta de firmware del servidor.
- Asegúrese de que el volumen NFS se exporte mediante NFS por medio de TCP.
- Asegúrese de que el servidor NAS exporte un recurso compartido determinado, como NFS 3 o NFS 4.1. El servidor NAS no debe proporcionar ambas versiones del protocolo para el mismo recurso compartido. El servidor NAS debe aplicar esta directiva, ya que ESXi no impide el montaje del mismo recurso compartido en diferentes versiones de NFS.
- NFS 3 y la versión NFS 4.1 que no pertenece a Kerberos (AUTH_SYS) no admiten la funcionalidad de usuarios delegados que permite el acceso a volúmenes NFS mediante credenciales no raíz. Si usa NFS 3 o la versión NFS 4.1 que no pertenece a Kerberos, asegúrese de que todos los hosts tengan acceso de raíz al volumen. Los diferentes proveedores de almacenamiento tienen diferentes métodos para habilitar esta funcionalidad, pero generalmente los servidores NAS usan la opción `no_root_squash`. Si el servidor NAS no otorga acceso de raíz, aún se puede montar el almacén de datos NFS en el host. Sin embargo, no se pueden crear máquinas virtuales en el almacén de datos.

- Si el volumen NFS subyacente es de solo lectura, asegúrese de que el servidor NFS exporte el volumen como recurso compartido de solo lectura. Como alternativa, se puede montar el volumen como almacén de datos de solo lectura en el host ESXi. De lo contrario, el host considerará que el almacén de datos es de lectura y escritura y no abrirá los archivos.

Redes en NFS

Un host ESXi usa la conexión de red TCP/IP para acceder a un servidor NAS remoto. Existen algunas directrices y prácticas recomendadas para configurar las redes cuando se utiliza el almacenamiento NFS.

Para obtener más información, consulte la documentación sobre *Redes de vSphere*.

- Para lograr conectividad de red, utilice un adaptador de red estándar en el host ESXi.
- ESXi admite conmutadores de red de Capa 2 y Capa 3. Si usa conmutadores de Capa 3, los hosts ESXi y las matrices de almacenamiento NFS deben estar en diferentes subredes y el conmutador de red debe controlar la información de enrutamiento.
- Configure un grupo de puertos de VMkernel para el almacenamiento NFS. Puede crear el grupo de puertos de VMkernel para el almacenamiento IP en un conmutador virtual (vSwitch) existente o en un vSwitch nuevo. El vSwitch puede ser un conmutador estándar de vSphere (VSS) o vSphere Distributed Switch (VDS).
- Si usa varios puertos para el tráfico NFS, asegúrese de configurar correctamente los conmutadores virtuales y los conmutadores físicos.
- NFS 3 y NFS 4.1 admiten IPv6.

Bloqueo de archivos NFS

Los mecanismos de bloqueo de archivos permiten restringir el acceso a los datos almacenados en un servidor únicamente a un usuario o proceso por vez. Los mecanismos de bloqueo de las dos versiones de NFS no son compatibles. NFS 3 utiliza un bloqueo de propiedad y NFS 4.1 utiliza el bloqueo especificado del protocolo nativo.

El bloqueo de NFS 3 en ESXi no utiliza el protocolo Network Lock Manager (NLM). En cambio, VMware ofrece su propio protocolo de bloqueo. Para implementar los bloqueos de NFS 3, se crean archivos de bloqueo en el servidor NFS. Los archivos de bloqueo se llaman `.lck-`*`file_id`*.

NFS 4.1 utiliza reservas de recursos compartidos como mecanismo de bloqueo.

Como los clientes de NFS 3 y NFS 4.1 no usan el mismo protocolo de bloqueo, no se pueden utilizar diferentes versiones de NFS para montar el mismo almacén de datos en varios hosts. Si se accede a los mismos discos virtuales desde dos clientes incompatibles, se puede producir un comportamiento incorrecto y los datos pueden dañarse.

Seguridad de NFS

Con NFS 3 y NFS 4.1, ESXi es compatible con el sistema de seguridad AUTH_SYS. Además, para NFS 4.1, también se admite el mecanismo de seguridad Kerberos.

NFS 3 es compatible con el mecanismo de seguridad AUTH_SYS. Con este mecanismo, el tráfico de almacenamiento se transmite por la LAN en un formato sin cifrar. Debido a esta seguridad limitada, utilice el almacenamiento NFS solo en redes de confianza y aísle el tráfico en conmutadores físicos individuales. También puede utilizar una VLAN privada.

NFS 4.1 admite el protocolo de autenticación Kerberos para proteger las comunicaciones con el servidor NFS. Los usuarios no raíz pueden acceder a los archivos si se utiliza Kerberos. Para obtener más información, consulte Usar Kerberos para NFS 4.1.

Además de Kerberos, NFS 4.1 admite los montajes tradicionales que no pertenecen a Kerberos con el mecanismo de seguridad AUTH_SYS. En este caso, siga las directrices de acceso de raíz para la versión 3 de NFS.

Nota No se pueden usar dos mecanismos de seguridad, AUTH_SYS y Kerberos, para el mismo almacén de datos NFS 4.1 compartido por varios hosts.

Uso de múltiples rutas en NFS

NFS 4.1 admite múltiples rutas en función de las especificaciones del protocolo. Para NFS 3, no se pueden aplicar las múltiples rutas.

NFS 3 utiliza una conexión TCP de E/S. En consecuencia, ESXi admite la E/S solo en una dirección IP o un nombre de host del servidor NFS, y no admite múltiples rutas de acceso. Según la infraestructura y la configuración de la red, puede utilizar la pila de red para configurar varias conexiones con los destinos de almacenamiento. En este caso, debe tener varios almacenes de datos, y cada uno de ellos debe utilizar conexiones de red individuales entre el host y el almacenamiento.

NFS 4.1 ofrece múltiples rutas para los servidores que admiten el enlace troncal de sesiones. Cuando el enlace troncal está disponible, se pueden utilizar varias direcciones IP para acceder a un solo volumen NFS. No se admite el enlace troncal del identificador de cliente.

NFS y aceleración de hardware

Los discos virtuales creados en los almacenes de datos NFS reciben aprovisionamiento fino de forma predeterminada. Para poder crear discos virtuales con aprovisionamiento grueso, es necesario utilizar una aceleración de hardware que admita la operación de reserva de espacio.

NFS 3 y NFS 4.1 admiten la aceleración de hardware para permitir que el host se integre con los dispositivos NAS y utilice varias operaciones de hardware que ofrece el almacenamiento NAS. Para obtener más información, consulte Aceleración de hardware en dispositivos NAS.

Almacenes de datos NFS

Al crear un almacén de datos NFS, recuerde seguir las directrices específicas.

Las directrices y prácticas recomendadas para los almacenes de datos NFS incluyen los siguientes puntos:

- No se pueden utilizar diferentes versiones de NFS para montar el mismo almacén de datos en distintos hosts. Los clientes de NFS 3 y NFS 4.1 no son compatibles y no usan el mismo protocolo de bloqueo. Como resultado, si se accede a los mismos discos virtuales desde dos clientes no compatibles, se puede producir un comportamiento incorrecto y los datos pueden dañarse.
- Los almacenes de datos NFS 3 y NFS 4.1 pueden coexistir en el mismo host.
- ESXi no puede actualizar automáticamente la versión 3 de NFS a la versión 4.1, pero es posible utilizar otros métodos de conversión. Para obtener información, consulte Protocolos NFS y ESXi.
- Al montar el mismo volumen NFS 3 en diferentes hosts, compruebe que los nombres de servidor y carpeta sean idénticos en todos los hosts. Si los nombres no coinciden, los hosts verán el mismo volumen NFS versión 3 como dos almacenes de datos diferentes. Este error puede provocar que características como vMotion no funcionen correctamente. Un ejemplo de esta discrepancia consiste en la introducción de `filer` como el nombre del servidor en un host y `filer.domain.com` en el otro. Esta instrucción no se aplica a la versión 4.1 de NFS.
- Si utiliza caracteres no ASCII para nombrar almacenes de datos y máquinas virtuales, asegúrese de que el servidor NFS subyacente ofrezca compatibilidad de internacionalización. Si el servidor no admite caracteres internacionales, use solo caracteres ASCII. De lo contrario, se producirán errores inesperados.

Configuraciones de firewall para almacenamiento NFS

ESXi incluye un firewall entre la interfaz de administración y la red. El firewall está habilitado de manera predeterminada. En el momento de la instalación, el firewall de ESXi está configurado para bloquear el tráfico entrante y saliente, a excepción del tráfico de los servicios predeterminados, como NFS.

Los servicios compatibles, incluido NFS, se describen en un archivo de configuración de un conjunto de reglas en el directorio `/etc/vmware/firewall/` del firewall de ESXi. El archivo contiene reglas de firewall y sus relaciones con puertos y protocolos.

El comportamiento del conjunto de reglas del cliente NFS (`nfsClient`) es diferente a otros conjuntos de reglas.

Para obtener más información sobre las configuraciones del firewall, consulte la documentación de *Seguridad de vSphere*.

Comportamiento de firewall del cliente NFS

El conjunto de reglas de firewall del cliente NFS se comporta de forma diferente a otros conjuntos de reglas de firewall de ESXi. ESXi configura los parámetros del cliente NFS cuando se monta o desmonta una almacén de datos de NFS. El comportamiento varía según la versión de NFS.

Cuando se agrega, monta o desmonta un almacén de datos de NFS, el comportamiento que se obtiene varía según la versión de NFS.

Comportamiento de firewall de NFS v3

Cuando se agrega o monta un almacén de datos de NFS v3, ESXi comprueba el estado del conjunto de reglas de firewall del cliente NFS (`nfsClient`).

- Si el conjunto de reglas `nfsClient` está deshabilitado, ESXi habilita el conjunto de reglas y deshabilita la directiva Permitir todas las direcciones IP estableciendo la marca `allowedAll` en `FALSE`. La dirección IP del servidor NFS se agrega a la lista de direcciones IP salientes permitidas.
- Si el conjunto de reglas `nfsClient` está habilitado, el estado del conjunto de reglas y la directiva de direcciones IP permitidas no se cambian. La dirección IP del servidor NFS se agrega a la lista de direcciones IP salientes permitidas.

Nota Si habilita manualmente el conjunto de reglas `nfsClient` o configura manualmente la directiva Permitir todas las direcciones IP, ya sea antes o después de agregar un almacén de datos de NFS v3 al sistema, la configuración se anula cuando se desmonta el último almacén de datos de NFS v3. El conjunto de reglas `nfsClient` se deshabilita cuando se desmontan todos los almacenes de datos de NFS v3.

Cuando se quita o se desmonta un almacén de datos de NFS v3, ESXi realiza una de las siguientes acciones.

- Si ninguno de los almacenes de datos de NFS v3 restantes se monta desde el servidor del almacén de datos que se desmonta, ESXi quita la dirección IP del servidor de la lista de direcciones IP salientes.
- Si ninguno de los almacenes de datos de NFS v3 permanece después de la operación de desmontaje, ESXi deshabilita el conjunto de reglas de firewall de `nfsClient`.

Comportamiento de firewall de NFS v4.1

Cuando se monta el primer almacén de datos NFS v4.1, ESXi habilita el conjunto de reglas `nfs41client` y establece su marca `allowedAll` en TRUE. Esta acción abre el puerto 2049 para todas las direcciones IP. Cuando se desmonta el almacén de datos NFS v4.1, el estado del firewall no se ve afectado. De esta forma, el primer montaje de NFS v4.1 abre el puerto 2049, y ese puerto permanece habilitado a menos que se cierre explícitamente.

Comprobar los puertos de firewall para clientes NFS

Para habilitar el acceso al almacenamiento NFS, ESXi abre automáticamente puertos de firewall para los clientes NFS cuando se monta un almacén de datos NFS. Por motivos de solución de problemas, es posible que deba comprobar que los puertos estén abiertos.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Sistema**, haga clic en **Firewall** y en **Editar**.

4 Desplácese hacia abajo hasta la versión correspondiente de NFS para asegurarse de que el puerto esté abierto.

Usar las conexiones enrutadas de Capa 3 para acceder al almacenamiento NFS

Cuando utilice conexiones enrutadas de Capa 3 (L3) para acceder al almacenamiento NFS, debe tener en cuenta ciertos requisitos y restricciones.

Asegúrese de que el entorno cumpla los siguientes requisitos:

- Utilice el protocolo Hot Standby Router (HSRP) de Cisco en un enrutador IP. Si utiliza un enrutador de otra marca, use el protocolo Virtual Router Redundancy Protocol (VRRP).
- Para priorizar el tráfico de Capa 3 de NFS en redes con ancho de banda limitado, o en redes que experimentan congestiones, utilice la calidad de servicio (QoS). Para obtener detalles, consulte la documentación del enrutador.
- Siga las recomendaciones de conexiones enrutadas de Capa 3 de NFS que ofrece el proveedor de almacenamiento. Para obtener detalles, póngase en contacto con el proveedor de almacenamiento.
- Deshabilite la administración de recursos de E/S de la red (NetIORM).
- Si piensa usar sistemas con conmutadores ubicados en la parte superior del bastidor o de la partición de dispositivos de E/S que dependen del conmutador, póngase en contacto con el proveedor del sistema para obtener información sobre compatibilidad y soporte.

En un entorno de Capa 3, se aplican las siguientes restricciones:

- El entorno no admite VMware Site Recovery Manager.
- El entorno admite únicamente el protocolo NFS. No use otros protocolos de almacenamiento, como FCoE, en la misma red física.
- El tráfico NFS en este entorno no es compatible con IPv6.
- El tráfico NFS en este entorno puede enrutarse solo a través de una LAN. No existe compatibilidad con otros entornos como WAN.

Usar Kerberos para NFS 4.1

Con la versión 4.1 de NFS, ESXi admite el mecanismo de autenticación Kerberos.

El mecanismo RPCSEC_GSS Kerberos es un servicio de autenticación. Permite instalar un cliente de NFS 4.1 en ESXi para probar su identidad en un servidor NFS antes de montar un recurso compartido de NFS. La seguridad Kerberos utiliza criptografía para funcionar en una conexión de red no segura.

La implementación de ESXi de Kerberos para NFS 4.1 proporciona dos modelos de seguridad, krb5 y krb5i, que ofrecen distintos niveles de seguridad.

- Kerberos para autenticación solamente (krb5) admite la comprobación de identidad.
- Kerberos para autenticación e integridad de datos (krb5i), además de la comprobación de identidad, proporciona servicios de integridad de datos. Estos servicios ayudan a proteger el tráfico de NFS para evitar la alteración mediante la comprobación de posibles modificaciones en los paquetes de datos.

Kerberos admite algoritmos de cifrado que evitan que los usuarios no autorizados puedan acceder al tráfico de NFS. El cliente NFS 4.1 en ESXi intenta usar el algoritmo AES256-CTS-HMAC-SHA1-96 o AES128-CTS-HMAC-SHA1-96 para acceder a un recurso compartido en el servidor NAS. Antes de utilizar los almacenes de datos de NFS 4.1, asegúrese de que AES256-CTS-HMAC-SHA1-96 o AES128-CTS-HMAC-SHA1-96 estén habilitados en el servidor NAS.

En la siguiente tabla, se comparan los niveles de seguridad de Kerberos admitidos por ESXi.

Tabla 17-5. Tipos de seguridad de Kerberos

		ESXi 6.0	ESXi 6.5 y versiones posteriores
Kerberos para autenticación solamente (krb5)	Suma de comprobación de integridad para encabezado RPC	Sí con DES	Sí con AES
	Comprobación de integridad para datos de RPC	No	No
Kerberos para autenticación e integridad de datos (krb5i)	Suma de comprobación de integridad para encabezado RPC	Sin krb5i	Sí con AES
	Comprobación de integridad para datos de RPC		Sí con AES

Al utilizar la autenticación Kerberos, se deben tener en cuenta las siguientes consideraciones:

- ESXi utiliza Kerberos con el dominio de Active Directory.
- Como administrador de vSphere, debe especificar credenciales de Active Directory para proporcionar acceso a un usuario de NFS a los almacenes de datos Kerberos de NFS 4.1. Se utiliza un único conjunto de credenciales para acceder a todos los almacenes de datos Kerberos montados en ese host.
- Cuando varios hosts ESXi comparten el almacén de datos NFS 4.1, se deben utilizar las mismas credenciales de Active Directory para todos los hosts que tienen acceso al almacén de datos compartido. Para automatizar el proceso de asignación, establezca el usuario en los perfiles de host y aplique el perfil a todos los hosts ESXi.
- No se pueden usar dos mecanismos de seguridad, AUTH_SYS y Kerberos, para el mismo almacén de datos NFS 4.1 compartido por varios hosts.

Configurar entorno de almacenamiento NFS

Se deben realizar varios pasos de configuración antes de montar un almacén de datos NFS en vSphere.

Requisitos previos

- Familiarícese con las instrucciones en Instrucciones y requisitos de almacenamiento NFS.
- Para obtener detalles sobre la configuración del almacenamiento NFS, consulte la documentación del proveedor de almacenamiento.
- Si utiliza Kerberos, asegúrese de que AES256-CTS-HMAC-SHA1-96 o AES128-CTS-HMAC-SHA1-96 estén habilitados en el servidor NAS.

Procedimiento

1. En el servidor NFS, configure un volumen NFS y expórtelo para montarlo en los hosts ESXi.
   a. Tome nota de la dirección IP o del nombre DNS del servidor NFS y de la ruta de acceso completa, o del nombre de carpeta, del recurso compartido de NFS.

      En NFS 4.1 se pueden recopilar varias direcciones IP o nombres de DNS para utilizar la compatibilidad con múltiples rutas que proporciona el almacén de datos NFS 4.1.
   b. Si planifica utilizar la autenticación Kerberos con NFS 4.1, especifique las credenciales Kerberos que utilizará ESXi para la autenticación.
2. En cada host ESXi, configure un puerto de red del VMkernel para el tráfico NFS.

   Para obtener más información, consulte la documentación sobre *Redes de vSphere*.
3. Si planifica utilizar la autenticación Kerberos con el almacén de datos NFS 4.1, configure los hosts ESXi para la autenticación Kerberos.

   Consulte Configurar hosts ESXi para la autenticación Kerberos.

Pasos siguientes

Ahora puede crear un almacén de datos NFS en los hosts ESXi.

Configurar hosts ESXi para la autenticación Kerberos

Si utiliza NFS 4.1 con Kerberos, debe realizar varias tareas para configurar los hosts para la autenticación Kerberos.

Cuando varios hosts ESXi comparten el almacén de datos NFS 4.1, se deben utilizar las mismas credenciales de Active Directory para todos los hosts que tienen acceso al almacén de datos compartido. Para automatizar el proceso de asignación, configure el usuario en los perfiles de host y aplique el perfil a todos los hosts ESXi.

Requisitos previos

- Asegúrese de que los servidores de Microsoft Active Directory (AD) y NFS estén configurados para utilizar Kerberos.

- Habilite los modos de cifrado AES256-CTS-HMAC-SHA1-96 o AES128-CTS-HMAC-SHA1-96 en AD. El cliente NFS 4.1 no es compatible con el modo de cifrado DES-CBC-MD5.
- Asegúrese de que las exportaciones del servidor NFS estén configuradas para otorgar acceso completo al usuario de Kerberos.

Procedimiento

1 Configurar DNS para NFS 4.1 con Kerberos

   Cuando usa NFS 4.1 con Kerberos, debe cambiar la configuración de DNS en los hosts ESXi. La configuración debe apuntar al servidor DNS que está configurado para distribuir registros de DNS para el centro de distribución de claves (Key Distribution Center, KDC) de Kerberos. Por ejemplo, utilice la dirección del servidor de Active Directory si AD se utiliza como servidor DNS.

2 Configurar protocolo Network Time Protocol para NFS 4.1 con Kerberos

   Si utiliza NFS 4.1 con Kerberos, los hosts ESXi, el servidor NFS y el servidor de Active Domain deben tener la hora sincronizada. Por lo general, en la configuración, el servidor de Active Domain se utiliza como el servidor del protocolo de hora de red (Network Time Protocol, NTP).

3 Habilitar la autenticación Kerberos en Active Directory

   Si se utiliza almacenamiento NFS 4.1 con Kerberos, se debe agregar cada host ESXi a un dominio de Active Directory y habilitar la autenticación Kerberos. Kerberos se integra con Active Directory para habilitar el inicio de sesión único y proporciona una capa adicional de seguridad cuando se utiliza en una conexión de red que no es segura.

Pasos siguientes

Después de configurar el host para Kerberos, puede crear un almacén de datos NFS 4.1 con Kerberos habilitado.

Configurar DNS para NFS 4.1 con Kerberos

Cuando usa NFS 4.1 con Kerberos, debe cambiar la configuración de DNS en los hosts ESXi. La configuración debe apuntar al servidor DNS que está configurado para distribuir registros de DNS para el centro de distribución de claves (Key Distribution Center, KDC) de Kerberos. Por ejemplo, utilice la dirección del servidor de Active Directory si AD se utiliza como servidor DNS.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Redes**, haga clic en **Configuración de TCP/IP**.

4 Seleccione **Predeterminado** y haga clic en el icono **Editar**.

5 Introduzca manualmente la configuración de DNS.

Opción	Descripción
Dominio	*Nombre del dominio de AD*
Servidor DNS preferido	*IP del servidor de AD*
Dominios de búsqueda	*Nombre del dominio de AD*

Configurar protocolo Network Time Protocol para NFS 4.1 con Kerberos

Si utiliza NFS 4.1 con Kerberos, los hosts ESXi, el servidor NFS y el servidor de Active Domain deben tener la hora sincronizada. Por lo general, en la configuración, el servidor de Active Domain se utiliza como el servidor del protocolo de hora de red (Network Time Protocol, NTP).

La siguiente tarea describe cómo sincronizar el host de ESXi con el servidor NTP.

La práctica recomendada es usar el servidor de Active Domain como servidor NTP.

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Sistema**, seleccione **Configuración de hora**.
4. Haga clic en **Editar** y configure el servidor NTP.
   a. Seleccione **Usar protocolo de hora de red (Habilitar el cliente NTP)**.
   b. Para sincronizar con el servidor NTP, introduzca sus direcciones IP.
   c. Seleccione **Iniciar servicio NTP**.
   d. Establezca la directiva de inicio del servicio NTP.
5. Haga clic en **Aceptar**.

   El host se sincroniza con el servidor NTP.

Habilitar la autenticación Kerberos en Active Directory

Si se utiliza almacenamiento NFS 4.1 con Kerberos, se debe agregar cada host ESXi a un dominio de Active Directory y habilitar la autenticación Kerberos. Kerberos se integra con Active Directory para habilitar el inicio de sesión único y proporciona una capa adicional de seguridad cuando se utiliza en una conexión de red que no es segura.

Requisitos previos

Configure un dominio de AD y una cuenta de administrador de dominio con los derechos para agregar hosts al dominio.

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Sistema**, haga clic en **Servicios de autenticación**.

4 Agregue el host ESXi a un dominio de Active Directory.

   a En el panel Servicios de autenticación, haga clic en **Unirse al dominio**.

   b Proporcione la configuración del dominio y haga clic en **Aceptar**.

   El tipo de servicios de directorio cambia a Active Directory.

5 Configure o edite las credenciales de un usuario Kerberos de NFS.

   a En el panel Credenciales de Kerberos de NFS, haga clic en **Editar**.

   b Escriba un nombre de usuario y contraseña.

      Con estas credenciales se accede a los archivos almacenados en todos los almacenes de datos Kerberos.

   El estado de las credenciales Kerberos de NFS cambia a Habilitado.

Recopilar información estadística para el almacenamiento NFS

Puede usar la herramienta `nfsStats` en el host ESXi para mostrar información estadística sobre las llamadas de NFS y las llamadas de procedimiento remoto (RPC). El comando muestra información estadística de los montajes de NFS 3 y NFS 4.1 en el host ESXi.

Por lo general, la herramienta `nfsStats` realiza las siguientes tareas.

- Recopila estadísticas de NFS para investigar problemas cuando se implementa una nueva configuración, como un nuevo servidor o red NFS, en el entorno de NFS.
- Proporciona estadísticas sobre los éxitos y errores de las operaciones de NFS.
- Publica estadísticas de latencia sobre los éxitos y errores de las operaciones de NFS.
- Soluciona problemas de rendimiento de NFS.

La sintaxis del comando es `nfsStats` *opciones*.

Están disponibles las opciones de comando siguientes.

Tabla 17-6. Comandos `nfsStats`

Opción de comando	Descripción
`No option`	Obtenga estadísticas de NFS y estadísticas de RPC para todos los almacenes de datos NFS.
`-3`	Muestra solo las estadísticas de NFS 3.
`-4`	Muestra solo las estadísticas de NFS 4,1.
`-n`	Muestra solo las estadísticas de NFS 3 y NFS 4.1.
`-r`	Muestra las estadísticas de RPC.

Tabla 17-6. Comandos `nfsStats` (continuación)

Opción de comando	Descripción
`-i` *intervalo*	Muestra estadísticas de NFS y de RPC en un intervalo igual al valor especificado en segundos. Por ejemplo, si el valor que introduce es 10, las estadísticas se actualizan cada 10 segundos.
`-v` *DSNAME1, DSNAME2, ...*	Muestra estadísticas de NFS y de RPC para todos los almacenes de datos NFS especificados. Utilice esta opción en combinación con el tipo de almacén de datos NFS, por ejemplo, -3 o -4.
`-j`	Muestra las estadísticas en formato JSON.

Crear almacenes de datos

Puede utilizar el asistente Nuevo almacén de datos para crear almacenes de datos. Según cómo sea su almacenamiento y cuáles sean sus necesidades de almacenamiento, puede crear un almacén de datos de VMFS, NFS o Virtual Volumes.

Un almacén de datos de vSAN se crea automáticamente cuando se habilita vSAN. Para obtener información, consulte el documento *Administrar VMware vSAN*.

También puede utilizar el asistente Nuevo almacén de datos para administrar copias del almacén de datos de VMFS.

- Crear un almacén de datos de VMFS

  Los almacenes de datos de VMFS sirven como repositorios para las máquinas virtuales. Los almacenes de datos de VMFS se pueden configurar en cualquier dispositivo de almacenamiento basado en SCSI que el host detecte, incluidos el canal de fibra, iSCSI y los dispositivos de almacenamiento local.

- Crear un almacén de datos NFS

  Puede utilizar el asistente **Nuevo almacén de datos** para montar un volumen NFS.

- Crear un almacén de datos de Virtual Volumes

  Puede utilizar el asistente **Nuevo almacén de datos** para crear un almacén de datos de Virtual Volumes.

Crear un almacén de datos de VMFS

Los almacenes de datos de VMFS sirven como repositorios para las máquinas virtuales. Los almacenes de datos de VMFS se pueden configurar en cualquier dispositivo de almacenamiento basado en SCSI que el host detecte, incluidos el canal de fibra, iSCSI y los dispositivos de almacenamiento local.

Requisitos previos

1 Instale y configure todos los adaptadores que requiere el almacenamiento.

2 Para detectar los dispositivos de almacenamiento agregados recientemente, vuelva a examinar. Consulte Operaciones para volver a examinar el almacenamiento.

3 Compruebe que los dispositivos de almacenamiento que planea usar para sus almacenes de datos estén disponibles. Consulte Características de los dispositivos de almacenamiento.

Procedimiento

1 En el navegador de objetos de vSphere Client, vaya hasta un host, un clúster o un centro de datos.

2 En el menú contextual, seleccione **Almacenamiento > Nuevo almacén de datos**.

3 Seleccione VMFS como el tipo de almacén de datos.

4 Escriba el nombre del almacén de datos y, si es necesario, seleccione la ubicación en la que colocará el almacén de datos.

   El sistema aplica un límite de 42 caracteres para el nombre del almacén de datos.

5 Seleccione el dispositivo que desea usar para el almacén de datos.

   Importante El dispositivo que seleccione no debe mostrar ningún valor en la columna Volumen de instantánea. Si aparece un valor, el dispositivo contiene una copia de un almacén de datos de VMFS existente. Para obtener información sobre cómo administrar copias de almacenes de datos, consulte Administrar almacenes de datos de VMFS duplicados.

6 Especifique la versión del almacén de datos.

Opción	Descripción
VMFS 6	Formato predeterminado en todos los hosts que admiten VMFS6. Los hosts ESXi 6.0 o de versiones anteriores no pueden reconocer el almacén de datos de VMFS6.
VMFS5	El almacén de datos de VMFS5 admite el acceso mediante hosts ESXi 6.7 o de versiones anteriores.

7 Defina los detalles de configuración para el almacén de datos.

Nota El tamaño mínimo necesario para un almacén de datos de VMFS6 es de 2 GB.

a Especifique la configuración de la partición.

Opción	Descripción
Utilizar todas las particiones disponibles	Dedica el disco completo a un solo almacén de datos de VMFS. Si se selecciona esta opción, se eliminan todos los sistemas de archivos y los datos almacenados en este dispositivo.
Utilizar espacio libre	Implementa un almacén de datos de VMFS en el espacio libre del disco.

b Si el espacio asignado para el almacén de datos es excesivo para el objetivo buscado, ajuste los valores de capacidad en el campo Tamaño del almacén de datos.

De manera predeterminada, se asigna todo el espacio libre en el dispositivo de almacenamiento.

c Para VMFS6, especifique el tamaño de bloque y defina los parámetros de recuperación de espacio. Consulte Solicitudes de recuperación de espacio de almacenes de datos de VMFS.

8 En la página Listo para finalizar, revise la información de configuración del almacén de datos y haga clic en **Finalizar**.

Resultados

Se crea el almacén de datos en el dispositivo de almacenamiento basado en SCSI. Está disponible para todos los hosts que tienen acceso al dispositivo.

Pasos siguientes

Después de crear el almacén de datos de VMFS, puede realizar las siguientes tareas:

- Cambie la capacidad del almacén de datos. Consulte Aumentar la capacidad de un almacén de datos de VMFS.
- Edite la configuración de recuperación de espacio. Consulte Cambiar la configuración de recuperación de espacio.
- Habilite la compatibilidad con VMDK compartido. Consulte Habilitar o deshabilitar la compatibilidad con discos virtuales agrupados en clúster en el almacén de datos VMFS6.

Crear un almacén de datos NFS

Puede utilizar el asistente **Nuevo almacén de datos** para montar un volumen NFS.

Requisitos previos

- Configure el entorno de almacenamiento NFS.

- Si desea utilizar la autenticación Kerberos con el almacén de datos NFS 4.1, asegúrese de configurar los hosts ESXi para la autenticación Kerberos.

Procedimiento

1 En el navegador de objetos de vSphere Client, vaya hasta un host, un clúster o un centro de datos.

2 En el menú contextual, seleccione **Almacenamiento > Nuevo almacén de datos**.

3 Seleccione NFS como el tipo de almacén de datos y especifique una versión de NFS.

   - NFS 3
   - NFS 4.1

   Importante Si varios hosts acceden al mismo almacén de datos, debe utilizar el mismo protocolo en todos los hosts.

4 Introduzca los parámetros del almacén de datos.

Opción	Descripción
Nombre de almacén de datos	El sistema aplica un límite de 42 caracteres para el nombre del almacén de datos.
Carpeta	El nombre de carpeta del punto de montaje.
Server	El nombre o la dirección IP del servidor. Puede usar formatos IPv6 o IPv4. Con NFS 4.1, puede agregar varias direcciones IP o nombres de servidores si el servidor NFS admite el enlace troncal. El host ESXi utiliza estos valores para lograr la habilitación de múltiples rutas al punto de montaje del servidor NFS.

5 Seleccione **Montar NFS de solo lectura** si el servidor NFS exporta el volumen como de solo lectura.

6 Para utilizar el mecanismo de seguridad de Kerberos con NFS 4.1, habilite Kerberos y seleccione un modelo de Kerberos apropiado.

Opción	Descripción
Usar Kerberos para autenticación solamente (krb5)	Admite la verificación de identidad.
Usar Kerberos para autenticación e integridad de datos (krb5i)	Además de la verificación de identidad, proporciona servicios de integridad de datos. Estos servicios ayudan a proteger el tráfico de NFS para evitar la alteración mediante la comprobación de posibles modificaciones en los paquetes de datos.

   Si no habilita Kerberos, el almacén de datos usa el mecanismo de seguridad AUTH_SYS predeterminado.

7 Si está creando un almacén de datos en el nivel del clúster o del centro de datos, seleccione los hosts que montan el almacén de datos.

8 Revise las opciones de configuración y haga clic en **Finalizar**.

Crear un almacén de datos de Virtual Volumes

Puede utilizar el asistente **Nuevo almacén de datos** para crear un almacén de datos de Virtual Volumes.

Procedimiento

1 En el navegador de objetos de vSphere Client, vaya hasta un host, un clúster o un centro de datos.

2 En el menú contextual, seleccione **Almacenamiento > Nuevo almacén de datos**.

3 Seleccione **vVol** como tipo de almacén de datos.

4 Introduzca el nombre del almacén de datos y seleccione un contenedor de almacenamiento de respaldo en la lista de contenedores de almacenamiento.

   Asegúrese de utilizar un nombre que no duplique el de otro almacén de datos en el entorno del centro de datos.

   Si monta el mismo almacén de datos de Virtual Volumes en varios hosts, el nombre del almacén de datos debe ser uniforme entre todos los hosts.

5 Seleccione los hosts que requieren acceso al almacén de datos.

6 Revise las opciones de configuración y haga clic en **Finalizar**.

Pasos siguientes

Después de crear el almacén de datos de Virtual Volumes, puede realizar operaciones de almacenes de datos, como cambiar el nombre del almacén de datos, explorar los archivos del almacén de datos, desmontar el almacén de datos, etc.

No puede agregar el almacén de datos de Virtual Volumes a un clúster de almacenes de datos.

Administrar almacenes de datos de VMFS duplicados

Cuando un dispositivo de almacenamiento contiene una copia del almacén de datos de VMFS, se puede montar el almacén de datos con la firma existente o asignar una firma nueva.

Cada almacén de datos de VMFS creado en un dispositivo de almacenamiento tiene una firma única, también llamada "UUID", que se almacena en el superbloque del sistema de archivos. Cuando el dispositivo de almacenamiento se replica o su instantánea se crea del lado de la matriz, la copia de dispositivo que se produce es idéntica, byte por byte, al dispositivo original. Por ejemplo, si el dispositivo de almacenamiento original contiene un almacén de datos VMFS con UUIDX, parecerá que la copia contiene una copia del almacén de datos con el mismo UUIDX.

Además de las instantáneas y las replicaciones de LUN, ciertas operaciones del dispositivo, como cambios en el identificador de LUN, podrían producir una copia del almacén de datos original.

ESXi puede detectar la copia del almacén de datos de VMFS. Puede montar la copia del almacén de datos con su UUID original o cambiar el UUID. El proceso de cambio del UUID se conoce como volver a firmar un almacén de datos.

La elección entre volver a firmar o montar sin volver a firmar depende de cómo se enmascaran los LUN en el entorno de almacenamiento. Si los hosts pueden ver las dos copias del LUN, el método óptimo es volver a firmar.

Conservar la firma de almacén de datos existente

Si no se necesita volver a firmar una copia del almacén de datos de VMFS, se la puede montar sin cambiar la firma.

Se puede mantener la firma, por ejemplo, si se conservan copias sincronizadas de las máquinas virtuales en un sitio secundario como parte de un plan de recuperación ante desastres. En el caso de que ocurra un desastre en el sitio principal, se monta la copia del almacén de datos y se encienden las máquinas virtuales en el sitio secundario.

Volver a firmar una copia de un almacén de datos de VMFS

Utilice la opción para volver a firmar el almacén de datos si desea retener los datos almacenados en la copia del almacén de datos de VMFS.

Cuando vuelve a firmar una copia de VMFS, ESXi asigna una firma nueva (UUID) a la copia y monta la copia como un almacén de datos distinto del original. Se actualizan todas las referencias a la firma original en los archivos de configuración de máquina virtual.

Al volver a firmar un almacén de datos, tenga en cuenta los siguientes puntos:

- Volver a firmar un almacén de datos es una acción irreversible.
- Luego de volver a firmar, la réplica del dispositivo de almacenamiento que contenía la copia de VMFS ya no se trata como una réplica.
- Un almacén de datos extendido puede volver a firmarse solamente si todas sus extensiones están en línea.
- El proceso de volver a firmar tolera errores. Si el proceso se interrumpe, es posible reanudarlo más adelante.
- Puede montar el nuevo almacén de datos VMFS sin riesgo de que su UUID entre en conflicto con los UUID de otros almacenes de datos de la jerarquía de instantáneas de dispositivo.

Montar una copia de un almacén de datos de VMFS

Utilice la opción para volver a firmar el almacén de datos si desea retener los datos almacenados en la copia del almacén de datos de VMFS. Si no se necesita volver a firmar una copia del almacén de datos de VMFS, se puede montar sin cambiar la firma.

Requisitos previos

- Vuelva a examinar el almacenamiento en el host para actualizar la vista de los dispositivos de almacenamiento presentados al host.
- Desmonte el almacén de datos de VMFS original que tiene el mismo UUID que la copia que planifica montar. Puede montar la copia del almacén de datos de VMFS solo si no entra en conflicto con el almacén de datos de VMFS original.

Procedimiento

1 En el navegador de objetos de vSphere Client, vaya hasta un host, un clúster o un centro de datos.

2 En el menú contextual, seleccione **Almacenamiento > Nuevo almacén de datos**.

3 Seleccione VMFS como el tipo de almacén de datos.

4 Escriba el nombre del almacén de datos y, si es necesario, seleccione la ubicación en la que colocará el almacén de datos.

5 En la lista de dispositivos de almacenamiento, seleccione el dispositivo que tiene un valor específico en la columna Volumen de snapshot.

   El valor presente en la columna Volumen de snapshot indica que el dispositivo es una copia que contiene una copia de un almacén de datos de VMFS existente.

6 Monte el almacén de datos.

Opción	Descripción
Montar volviendo a firmar	En **Opciones de montaje**, seleccione **Asignar una nueva firma** y haga clic en **Siguiente**.
Montar sin volver a firmar	En Opciones de montaje, seleccione **Mantener firma existente**.

7 Revise la información de configuración del almacén de datos y haga clic en **Finalizar**.

Aumentar la capacidad de un almacén de datos de VMFS

La capacidad de un almacén de datos de VMFS se puede aumentar. Es posible que necesite más capacidad al agregar máquinas virtuales al almacén de datos o cuando las máquinas virtuales que se ejecutan en el almacén de datos requieren más espacio.

Si un almacén de datos compartido encendió máquinas virtuales y está totalmente lleno, es posible aumentar la capacidad del almacén de datos. Solo puede realizar esta acción en el host en el que están registradas las máquinas virtuales encendidas.

En función de la configuración de almacenamiento, puede utilizar uno de los siguientes métodos para aumentar la capacidad del almacén de datos. No es necesario apagar las máquinas virtuales al usar cualquiera de los métodos para aumentar la capacidad del almacén de datos.

Expandir un almacén de datos existente

Aumente el tamaño de un almacén de datos expandible. El almacén de datos se considera expandible cuando el dispositivo de almacenamiento de copia de seguridad tiene espacio disponible inmediatamente después de la extensión del almacén de datos.

Agregar una extensión

Aumente la capacidad de un almacén de datos de VMFS existente agregando nuevos dispositivos de almacenamiento al almacén de datos. El almacén de datos puede abarcar varios dispositivos de almacenamiento y aún mostrarse como un solo volumen.

El almacén de datos de VMFS expandido puede utilizar cualquiera de las extensiones o todas ellas en cualquier momento. No es necesario que complete una extensión en especial para poder utilizar la siguiente.

Nota Los almacenes de datos que admiten solo bloqueo asistido por hardware, también denominado mecanismo ATS, no pueden expandirse a dispositivos sin bloqueo con ATS. Para obtener más información, consulte Mecanismos de bloqueo de VMFS.

Requisitos previos

Puede aumentar la capacidad del almacén de datos si el almacenamiento del host cumple con una de las siguientes condiciones:

- El dispositivo de copia de seguridad del almacén de datos existente tiene suficiente espacio disponible.
- Se agregaron nuevos dispositivos de almacenamiento al host.

Procedimiento

1 En vSphere Client, desplácese al almacén de datos.

2 Seleccione **Aumentar capacidad del almacén de datos** en el menú contextual del almacén de datos.

3 Seleccione un dispositivo de la lista de dispositivos de almacenamiento.

La selección depende de si hay disponible un dispositivo de almacenamiento ampliable.

Opción	Descripción
Para expandir una extensión de almacén de datos existente	Seleccione el dispositivo para el cual la columna Ampliable diga Sí.
Para agregar una extensión	Seleccione el dispositivo para el cual la columna Ampliable diga NO.

4 Revise el **Diseño de particiones** para ver las configuraciones disponibles.

5 Seleccione una opción de configuración del panel inferior.

Según el diseño actual del disco y las opciones que seleccionó anteriormente, pueden variar los elementos de menú que verá.

Elemento del menú	Descripción
Utilizar espacio libre para expandir el almacén de datos	Expande una extensión existente a la capacidad necesaria.
Utilizar espacio libre	Implementa una extensión en el espacio libre restante del disco. Este elemento de menú está disponible solo cuando agrega una extensión.
Utilizar todas las particiones disponibles	Dedica el disco completo a una sola extensión. Este elemento de menú está disponible solo cuando agrega una extensión y cuando el disco al que está dando formato no está vacío. Se reformatea el disco y se eliminan los almacenes de datos junto con los datos que contengan.

6 Establezca la capacidad de la extensión.

El tamaño mínimo de la extensión es de 1,3 GB. De forma predeterminada, todo el espacio libre en el dispositivo de almacenamiento está disponible.

7 Haga clic en **Siguiente**.

8 Revise el diseño propuesto y la configuración nueva del almacén de datos y haga clic en **Finalizar**.

Habilitar o deshabilitar la compatibilidad con discos virtuales agrupados en clúster en el almacén de datos VMFS6

Si tiene pensado utilizar un disco virtual en las configuraciones de clústeres de conmutación por error de Windows Server (WSFC), el almacén de datos de VMFS6 debe admitir discos virtuales agrupados en clúster. Utilice vSphere Client para habilitar la compatibilidad con discos agrupados en clúster.

Para obtener información sobre el uso de discos virtuales agrupados en clúster en clústeres de máquinas virtuales, consulte la documentación de *Configuración de clústeres de conmutación por error de Windows Server*.

Requisitos previos

Siga estas directrices cuando utilice un almacén de datos para discos virtuales agrupados en clúster:

- La matriz de almacenamiento debe ser compatible con el tipo de reserva de ATS, Write Exclusive – All Registrant (exclusivo de escritura y todos los inscritos, WEAR) SCSI-3.
- ESXi solo admite matrices de Fibre Channel para este tipo de configuraciones.
- Solo los almacenes de datos VMFS6 admiten discos agrupados en clúster. Los almacenes de datos que utilice no podrán expandirse ni abarcar varias extensiones.

- NMP debe reclamar los dispositivos de almacenamiento. ESXi no es compatible con los complementos de terceros (third-party plug-in, MPP) en las configuraciones de discos virtuales agrupados en clúster.
- Asegúrese de que los discos virtuales que utiliza para la agrupación en clústeres tengan el formato de puesta a cero rápida con aprovisionamiento grueso.

Procedimiento

1 En vSphere Client, desplácese al almacén de datos.

2 Haga clic en la pestaña **Configurar** y en **General**.

3 En **Capacidades de almacén de datos**, haga clic en una de las siguientes opciones junto al elemento **VMDK agrupado en clúster**.

Opción	Descripción
Habilitar	Para habilitar la compatibilidad con discos virtuales agrupados en clúster en el almacén de datos. Después de habilitar la compatibilidad, puede colocar los discos virtuales agrupados en clúster en este almacén de datos de VMFS.
Deshabilitar	Para deshabilitar la compatibilidad. Antes de deshabilitar, asegúrese de desconectar todas las máquinas virtuales con los discos virtuales agrupados en clúster.

4 Confirme su configuración.

Operaciones administrativas para almacenes de datos

Una vez creados los almacenes de datos, se pueden realizar varias operaciones administrativas en ellos. Ciertas operaciones, como el cambio de nombre de los almacenes de datos, están disponibles para todos los tipos de almacenes de datos. Otras aplican a tipos de almacenes de datos específicos.

- Cambiar nombre del almacén de datos

  Utilice vSphere Client para cambiar el nombre de un almacén de datos existente. Puede cambiar el nombre de un almacén de datos en el que se están ejecutando máquinas virtuales sin consecuencias negativas.

- Desmontar almacenes de datos

  Al desmontar un almacén de datos, este permanece intacto aunque ya no es visible desde los hosts especificados. El almacén de datos sigue apareciendo en otros hosts, donde permanece montado.

- Montar almacenes de datos

  Es posible montar un almacén de datos que se desmontó previamente. También puede montar un almacén de datos en hosts adicionales para transformarlo en un almacén de datos compartido.

- Quitar almacenes de datos de VMFS

  Se puede eliminar cualquier tipo de almacén de datos de VMFS, incluidas las copias que se hayan montado sin volver a firmar. Cuando se elimina un almacén de datos, este se destruye y desaparece de todos los hosts que tienen acceso al almacén de datos.

- Usar el explorador del almacén de datos

  Utilice el explorador de archivos del almacén de datos para administrar el contenido de los almacenes de datos. Puede examinar las carpetas y los archivos que se encuentran el almacén de datos. También puede usar el explorador para cargar archivos y ejecutar tareas administrativas en las carpetas y los archivos.

- Desactivar los filtros de almacenamiento

  Cuando se realizan operaciones de administración de almacenes de datos de VMFS, vCenter Server utiliza los filtros predeterminados de protección de almacenamiento. Los filtros ayudan a evitar daños en el almacenamiento al recuperar solo los dispositivos de almacenamiento que se pueden utilizar para una operación determinada. Los dispositivos que no son adecuados no se pueden seleccionar porque no se muestran. Para ver todos los dispositivos, puede desactivar los filtros.

Cambiar nombre del almacén de datos

Utilice vSphere Client para cambiar el nombre de un almacén de datos existente. Puede cambiar el nombre de un almacén de datos en el que se están ejecutando máquinas virtuales sin consecuencias negativas.

Nota Si vCenter Server administra el host, no se puede cambiar el nombre del almacén de datos accediendo directamente al host desde VMware Host Client. Debe cambiar el nombre del almacén de datos en vCenter Server.

Procedimiento

1. En vSphere Client, desplácese al almacén de datos.
2. Haga clic con el botón derecho en el almacén de datos cuyo nombre desea cambiar y seleccione **Cambiar nombre**.
3. Escriba un nombre nuevo para el almacén de datos.

   El sistema aplica un límite de 42 caracteres para el nombre del almacén de datos.

Resultados

El nombre nuevo aparecerá en todos los hosts que tienen acceso al almacén de datos.

Desmontar almacenes de datos

Al desmontar un almacén de datos, este permanece intacto aunque ya no es visible desde los hosts especificados. El almacén de datos sigue apareciendo en otros hosts, donde permanece montado.

No realice ninguna operación de configuración que pueda provocar operaciones de E/S en el almacén de datos mientras el desmontaje está en curso.

Nota Asegúrese de que los latidos de vSphere HA no usen el almacén de datos. Los latidos de vSphere HA no le impiden desmontar el almacén de datos. Sin embargo, si el almacén de datos se utiliza para los latidos, desmontarlo podría provocar que el host genere errores y reinicie todas las máquinas virtuales activas.

Requisitos previos

Cuando sea apropiado, antes de desmontar almacenes de datos, asegúrese de que se cumplan los siguientes requisitos previos:

- Ninguna máquina virtual debe residir en el almacén de datos.
- Storage DRS no administra el almacén de datos.
- Storage I/O Control debe estar deshabilitado para este almacén de datos.

Procedimiento

1. En vSphere Client, desplácese al almacén de datos.
2. Haga clic con el botón derecho en el almacén de datos y seleccione **Desmontar almacén de datos**.
3. Si se comparte el almacén de datos, seleccione los hosts desde los cuales se desmontará el almacén de datos.
4. Confirme que desea desmontar el almacén de datos.

Resultados

Después de desmontar un almacén de datos de VMFS de todos los hosts, el almacén de datos se marca como inactivo. Si desmonta un NFS o un almacén de datos de Virtual Volumes de todos los hosts, el almacén de datos desaparece del inventario. Puede montar el almacén de datos de VMFS desmontado. Para montar el NFS o el almacén de datos de Virtual Volumes que se quitó del inventario, use el asistente Nuevo almacén de datos.

Pasos siguientes

Si desmontó el almacén de datos de VMFS como parte de un procedimiento de eliminación de almacenamiento, ahora puede desconectar el dispositivo de almacenamiento que respalda el almacén de datos. Consulte Separar dispositivos de almacenamiento.

Montar almacenes de datos

Es posible montar un almacén de datos que se desmontó previamente. También puede montar un almacén de datos en hosts adicionales para transformarlo en un almacén de datos compartido.

Un almacén de datos de VMFS que se desmontó de todos los hosts permanece en el inventario, pero se marca como inaccesible. Consulte Desmontar almacenes de datos.

Puede usar esta tarea para montar el almacén de datos de VMFS en un host específico o en varios hosts.

Si desmontó un NFS o un almacén de datos de Virtual Volumes de todos los hosts, el almacén de datos desaparece del inventario. Para montar el NFS o el almacén de datos de Virtual Volumes que se quitó del inventario, use el asistente Nuevo almacén de datos.

Un almacén de datos de cualquier tipo que se desmonta de algunos hosts mientras está montado en otros, se muestra como activo en el inventario.

Procedimiento

1 En vSphere Client, desplácese al almacén de datos.

2 Haga clic con el botón derecho en el almacén de datos que desea montar y seleccione una de las opciones siguientes:

   - **Montar almacén de datos**
   - **Montar almacén de datos en hosts adicionales**

   Según el tipo de almacén de datos que use, verá una opción o la otra.

3 Seleccione los hosts que deben tener acceso al almacén de datos y haga clic en **Aceptar**.

4 Para obtener una lista de todos los hosts que comparten el almacén de datos, desplácese hasta el almacén de datos y haga clic en la pestaña **Hosts**.

Quitar almacenes de datos de VMFS

Se puede eliminar cualquier tipo de almacén de datos de VMFS, incluidas las copias que se hayan montado sin volver a firmar. Cuando se elimina un almacén de datos, este se destruye y desaparece de todos los hosts que tienen acceso al almacén de datos.

Nota La operación de eliminación del almacén de datos elimina de manera permanente todos los archivos asociados a las máquinas virtuales en el almacén de datos. Aunque es posible eliminar el almacén de datos sin necesidad de desmontar, es preferible que primero se desmonte el almacén de datos.

Requisitos previos

- Quite o migre todas las máquinas virtuales del almacén de datos.
- Desmonte el almacén de datos de todos los hosts.
- Deshabilite Storage DRS para el almacén de datos.
- Deshabilite Storage I/O Control para el almacén de datos.
- Asegúrese de que el almacén de datos no se use para los latidos de vSphere HA.

Procedimiento

1 En vSphere Client, desplácese al almacén de datos.

2 Haga clic con el botón derecho en el almacén de datos que desea quitar y seleccione **Eliminar almacén de datos**.

3 Confirme que desea quitar el almacén de datos.

Usar el explorador del almacén de datos

Utilice el explorador de archivos del almacén de datos para administrar el contenido de los almacenes de datos. Puede examinar las carpetas y los archivos que se encuentran el almacén de datos. También puede usar el explorador para cargar archivos y ejecutar tareas administrativas en las carpetas y los archivos.

Procedimiento

1 Abra el navegador del almacén de datos.

   a Muestre el almacén de datos en el inventario.

   b Haga clic con el botón derecho en el almacén de datos y seleccione **Examinar archivos**.

2 Para explorar el contenido del almacén de datos, desplácese hasta las carpetas y los archivos existentes.

3 Para ejecutar las tareas administrativas, puede usar diversos iconos y opciones.

Iconos y opciones	Descripciones
Cargar archivos	Cargar un archivo en el almacén de datos.
Cargar carpeta (disponible solo en vSphere Client)	Cargar una carpeta al almacén de datos.
Descargar	Descargar del almacén de datos.
Carpeta nueva	Crear una carpeta en el almacén de datos.
Copiar en	Copiar las carpetas o los archivos seleccionados en una ubicación nueva, ya sea en el mismo almacén de datos o en uno diferente.
Mover a	Mover las carpetas o los archivos seleccionados a una ubicación nueva, ya sea en el mismo almacén de datos o en uno diferente.
Cambiar nombre a	Cambiar el nombre de los archivos seleccionados.
Suprimir	Eliminar las carpetas o los archivos seleccionados.
Expandir	Convertir un disco virtual fino seleccionado en disco grueso. Esta opción solo se aplica a discos con aprovisionamiento fino.

Cargar archivos o carpetas a almacenes de datos

Use el explorador de archivos de almacenes de datos para cargar archivos a almacenes de datos en el host ESXi. Si utiliza vSphere Client, también puede cargar carpetas.

Además de su uso tradicional como almacenamiento para archivos de máquinas virtuales, los almacenes de datos pueden servir para almacenar datos o archivos relacionados con máquinas virtuales. Por ejemplo, puede cargar imágenes ISO de sistemas operativos desde un equipo local a un almacén de datos en el host. A continuación, puede usar esas imágenes para instalar sistemas operativos invitados en las máquinas virtuales nuevas.

Nota No se pueden cargar archivos directamente a almacenes de datos de Virtual Volumes. Primero se debe crear una carpeta en el almacén de datos de Virtual Volumes para después poder cargar los archivos en la carpeta. Las carpetas creadas en los almacenes de datos de Virtual Volumes para almacenamiento en bloque tienen un espacio de capacidad de almacenamiento limitado de 4 GB. El almacén de datos de Virtual Volumes es compatible con cargas directas de carpetas.

Requisitos previos

Privilegio necesario: **Almacén de datos.Examinar almacén de datos**

Procedimiento

1. Abra el navegador del almacén de datos.
   a. Muestre el almacén de datos en el inventario.
   b. Haga clic con el botón derecho en el almacén de datos y seleccione **Examinar archivos**.
2. (opcional) Cree una carpeta para almacenar el archivo o la carpeta.
3. Cargue el archivo o la carpeta.

Opción	Descripción
Cargar un archivo	a Seleccione la carpeta de destino y haga clic en **Cargar archivos**. b Localice el elemento que desea cargar en el equipo local y haga clic en **Abrir**.
Cargar una carpeta (disponible solo en vSphere Client)	a Seleccione el almacén de datos o la carpeta de destino y haga clic en **Cargar carpeta**. b Localice el elemento que desea cargar en el equipo local y haga clic en **Aceptar**.

4. Actualice el explorador de archivos de almacenes de datos para ver los archivos o las carpetas cargados en la lista.

Pasos siguientes

Es posible que tenga problemas si implementa una plantilla de OVF que anteriormente se exportó y que después se cargó en el almacén de datos. Para obtener información detallada y una solución alternativa, consulte el artículo 2117310 de la base de conocimientos de VMware.

Descargar archivos de almacenes de datos

Use el explorador de archivos del almacén de datos para descargar en el equipo local los archivos del almacén de datos disponible en el host ESXi.

Requisitos previos

Privilegio necesario: **Almacén de datos.Examinar almacén de datos**

Procedimiento

1 Abra el navegador del almacén de datos.

   a Muestre el almacén de datos en el inventario.

   b Haga clic con el botón derecho en el almacén de datos y seleccione **Examinar archivos**.

2 Desplácese hasta el archivo que desea descargar y haga clic en **Descargar**.

3 Siga las indicaciones para guardar el archivo en el equipo local.

Mover o copiar archivos o carpetas del almacén de datos

Utilice el explorador del almacén de datos para mover o copiar las carpetas o los archivos a una ubicación nueva, ya sea en el mismo almacén de datos o en uno diferente.

Nota Los archivos de discos virtuales se mueven o copian sin conversión de formato. Si transfiere un disco virtual a un almacén de datos que pertenece a un host diferente del host de origen, es posible que necesite convertir el disco virtual. De lo contrario, quizás no pueda usar el disco.

No se pueden copiar archivos de máquina virtual de un vCenter Server a otro.

Requisitos previos

Privilegio necesario: **Almacén de datos.Examinar almacén de datos**

Procedimiento

1 Abra el navegador del almacén de datos.

   a Muestre el almacén de datos en el inventario.

   b Haga clic con el botón derecho en el almacén de datos y seleccione **Examinar archivos**.

2 Desplácese hasta el objeto que desea mover o copiar, ya sea una carpeta o un archivo.

3 Seleccione el objeto y haga clic en **Mover a** o en **Copiar a**.

4 Especifique la ubicación de destino.

5 (opcional) Seleccione **Sobrescribir archivos y carpetas con nombres coincidentes en el destino**.

6 Haga clic en **Aceptar**.

Cambiar el nombre de los archivos de almacén de datos

Utilice el explorador de almacenes de datos para cambiar el nombre de archivos.

Requisitos previos

Privilegio necesario: **Almacén de datos.Examinar almacén de datos**

Procedimiento

1 Abra el navegador del almacén de datos.

   a Muestre el almacén de datos en el inventario.

   b Haga clic con el botón derecho en el almacén de datos y seleccione **Examinar archivos**.

2 Desplácese hasta un archivo cuyo nombre desee cambiar.

3 Seleccione el archivo y haga clic en **Cambiar nombre a**.

4 Especifique el nombre nuevo y haga clic en **Aceptar**.

Expandir discos virtuales finos

Si creó un disco virtual en formato fino, puede cambiarlo a un formato grueso.

Puede utilizar el explorador de almacenes de datos para expandir el disco virtual fino.

Requisitos previos

- Asegúrese de que el almacén de datos donde se encuentra la máquina virtual tenga espacio suficiente.
- Asegúrese de que el disco virtual sea fino.
- Quite las instantáneas.
- Apague la máquina virtual.

Procedimiento

1 En vSphere Client, desplácese hasta la carpeta del disco virtual que desea expandir.

   a Desplácese hasta la máquina virtual.

   b Haga clic en la pestaña **Almacenes de datos**.

   Se enumera el almacén de datos que almacena los archivos de la máquina virtual.

   c Haga clic con el botón derecho en el almacén de datos y seleccione **Examinar archivos**.

   El explorador del almacén de datos muestra el contenido del almacén de datos.

2 Expanda la carpeta de la máquina virtual y desplácese hasta el archivo del disco virtual que desea convertir.

   El archivo tiene la extensión `.vmdk` y está marcado con el icono de disco virtual ().

3 Seleccione el archivo de disco virtual y haga clic en **Expandir**.

   Nota Es posible que la opción no esté disponible si el disco virtual es grueso o si la máquina virtual está en ejecución.

Resultados

El disco virtual inflado ocupa el espacio del almacén de datos completo que se le aprovisionó originalmente.

Desactivar los filtros de almacenamiento

Cuando se realizan operaciones de administración de almacenes de datos de VMFS, vCenter Server utiliza los filtros predeterminados de protección de almacenamiento. Los filtros ayudan a evitar daños en el almacenamiento al recuperar solo los dispositivos de almacenamiento que se pueden utilizar para una operación determinada. Los dispositivos que no son adecuados no se pueden seleccionar porque no se muestran. Para ver todos los dispositivos, puede desactivar los filtros.

Requisitos previos

Antes de cambiar los filtros de los dispositivos, consulte con el equipo de soporte de VMware.

Procedimiento

1 Desplácese hasta la instancia de vCenter Server.

2 Haga clic en la pestaña **Configurar**.

3 En **Configuración**, haga clic en **Configuración avanzada** y, a continuación, en **EDITAR CONFIGURACIÓN**.

4 Especifique el filtro que desea desactivar.

   En los cuadros de texto **Nombre** y **Valor** que aparecen en la parte inferior de la página, introduzca la información correspondiente.

Nombre	Valor
config.vpxd.filter.vmfsFilter	False
config.vpxd.filter.rdmFilter	False
config.vpxd.filter.sameHostsAndTransportsFilter	False
config.vpxd.filter.hostRescanFilter	False **Nota** Si se desactiva este filtro, los hosts continúan realizando nuevas exploraciones cada vez que se presenta un nuevo LUN ante un host o un clúster.

5 Haga clic en **AGREGAR** y, a continuación, en **GUARDAR** para guardar los cambios.

   No es necesario reiniciar el sistema vCenter Server.

Filtrado de almacenamiento

vCenter Server ofrece filtros de almacenamiento como ayuda para evitar daños o degradación del rendimiento en dispositivos de almacenamiento que pueden deberse a una utilización no admitida de esos dispositivos. Estos filtros están disponibles de forma predeterminada.

Tabla 17-7. Filtros de almacenamiento

Nombre del filtro	Descripción
config.vpxd.filter.vmfsFilter (Filtro de VMFS)	Filtra dispositivos de almacenamiento o LUN que un almacén de datos de VFMS ya utiliza en cualquier host administrado por vCenter Server. Los LUN no aparecen como candidatos para formatear con otro almacén de datos de VMFS o disponible para utilizarse como un RDM.
config.vpxd.filter.rdmFilter (Filtro de RDM)	Filtra los LUN que ya son utilizados como referencia por un RDM en cualquier host administrado por vCenter Server. Los LUN no aparecen como candidatos para formatearse con VMFS o para que un RDM diferente los utilice. Para que las máquinas virtuales accedan al mismo LUN, deben compartir el mismo archivo de asignación de RDM. Para obtener información sobre este tipo de configuración, consulte la documentación de *Administrar recursos de vSphere*.
config.vpxd.filter.sameHostsAndTransportsFilter (Filtro de mismo host y transportes)	Filtra los LUN que no cumplen los requisitos para ser utilizados como extensiones de almacenes de datos de VMFS debido a la incompatibilidad del host o del tipo de almacenamiento. Evita que agregue los siguientes LUN como extensiones: ■ LUN no expuesto a todos los hosts que comparten el almacén de datos de VMFS original. ■ LUN que utilizan un tipo de almacenamiento diferente del que utiliza el almacén de datos de VMFS original. Por ejemplo, no puede agregar una extensión de canal de fibra a un almacén de datos de VMFS en un dispositivo de almacenamiento local.
config.vpxd.filter.hostRescanFilter (Filtro para volver a examinar el host)	Vuelve a examinar y actualiza automáticamente almacenes de datos de VMFS después de realizar operaciones de administración de almacenes de datos. El filtro ayuda a contar con un panorama coherente de todos los almacenes de datos de VMFS en todos los hosts administrados por vCenter Server. **Nota** Si presenta un nuevo LUN a un host o un clúster, el host vuelve a examinarlo automáticamente, sin importar si el filtro para volver a examinar el host está activado o desactivado.

Configurar reflejo de discos dinámico

Generalmente, no se puede usar un software de administración de LUN en máquinas virtuales para reflejar discos virtuales. Sin embargo, si las máquinas virtuales de Microsoft Windows admiten discos dinámicos, se pueden reflejar discos virtuales en dos LUN de SAN. La creación de reflejo ayuda a proteger las máquinas virtuales contra una pérdida de dispositivos de almacenamiento no planificada.

Requisitos previos

- Use una máquina virtual de Windows que admita discos dinámicos.
- Privilegio necesario: **Máquina virtual. Configuración. Opciones**

Procedimiento

1 Cree una máquina virtual con dos discos virtuales.

Coloque los discos en diferentes almacenes de datos.

2 Inicie sesión en la máquina virtual y configure los discos como discos reflejados dinámicos.

Consulte la documentación de Microsoft.

3 Una vez sincronizados los discos, apague la máquina virtual.

4 Cambie la configuración de la máquina virtual para permitir la creación de reflejo del disco dinámico.

   a Haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.

   b Haga clic en la pestaña **Opciones de máquina virtual** y expanda el menú **Opciones avanzadas**.

   c Haga clic en **Editar configuración** junto a Parámetros de configuración.

   d Haga clic en **Agregar parámetros de configuración** y agregue los parámetros siguientes:

Nombre	Valor
`scsi#.returnNoConnectDuringAPD`	True
`scsi#.returnBusyOnNoConnectStatus`	False

   e Si utiliza ESXi 6.7 o una versión posterior, incluya un parámetro adicional para cada disco virtual que participa en la configuración de RAID-1 del software.

   Este parámetro evita errores de E/S del sistema operativo invitado cuando se produce un error en un dispositivo de almacenamiento.

Nombre	Valor
`scsi#:1.passthruTransientErrors`	True
`scsi#:2.passthruTransientErrors`	True

   f Haga clic en **Aceptar**.

Recopilar información de diagnóstico para hosts ESXi en un almacén de datos de VMFS

Durante un error del host, ESXi debe poder guardar la información de diagnóstico en una ubicación preconfigurada para fines de diagnóstico y soporte técnico.

Generalmente, durante la instalación de ESXi, se crea una partición en un dispositivo de almacenamiento local para recopilar información de diagnóstico, también conocida como volcado de núcleo. También puede configurar el recopilador de volcado de ESXi para que conserve los volcados de núcleo en un servidor de red. Para obtener información sobre cómo configurar el recopilador de volcado de ESXi, consulte la documentación de *Instalar y configurar VMware ESXi*.

Otra opción es usar un archivo en un almacén de datos de VMFS para recopilar la información de diagnóstico.

- Configurar un archivo como ubicación de volcado de núcleo

  Si el tamaño de la partición de volcado de núcleo disponible no es suficiente, puede configurar ESXi para que utilice un archivo en un almacén de datos de VMFS para obtener información de diagnóstico.

- Desactivar y eliminar un archivo de volcado de núcleo

  Desactive un archivo de volcado de núcleo configurado y, si es necesario, quítelo del almacén de datos de VMFS.

Configurar un archivo como ubicación de volcado de núcleo

Si el tamaño de la partición de volcado de núcleo disponible no es suficiente, puede configurar ESXi para que utilice un archivo en un almacén de datos de VMFS para obtener información de diagnóstico.

Nota Los almacenes de datos de VMFS en iSCSI de software no admiten archivos de volcado de núcleo.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 Cree un archivo para el volcado de núcleo del almacén de datos de VMFS con el comando siguiente:

  `esxcli system coredump file add`

  El comando toma las opciones siguientes, pero no son obligatorias y pueden omitirse:

Opción	Descripción
--auto | -a	Cree automáticamente un archivo si no se encuentra ninguno.
--datastore | -d *datastore_UUID o datastore_name*	Especifique el almacén de datos para el archivo de volcado. Si no se proporciona, el sistema selecciona un almacén de datos de tamaño suficiente.
--enable | -e	Habilite el archivo de diagnóstico después de la creación.
--file | -f *file_name*	Especifique el nombre de archivo del archivo de volcado. Si no se proporciona, el sistema crea un nombre único para el archivo.
--size |-s *file_size_MB*	Establezca el tamaño en MB del archivo de volcado. Si no se proporciona, el sistema crea un archivo del tamaño adecuado para la memoria instalada en el host.

2 Compruebe que se haya creado el archivo:

esxcli system coredump file list

Puede ver un resultado similar al siguiente:

```
Path                                              Active Configured Size
------------------------------------------------- ------ ---------- ---------
/vmfs/volumes/52b021c3-.../vmkdump/test.dumpfile false  false      104857600
```

3 Active el archivo para el volcado de núcleo para el host:

esxcli system coredump file set

El comando admite las siguientes opciones:

Opción	Descripción
--enable |-e	Habilite o deshabilite el archivo de volcado. No se puede especificar esta opción al anular la configuración del archivo de volcado.
--path | -p	La ruta de acceso del archivo para el volcado de núcleo que se usará. El archivo debe preasignarse.
--smart | -s	Esta marca solo se puede usar con **--enable | -e=true**. Hará que el archivo se seleccione con el algoritmo de selección inteligente. Por ejemplo, **esxcli system coredump file set --smart --enable true**
--unconfigure | -u	Anule la configuración del archivo de volcado actual de VMFS.

4 Compruebe que el archivo para el volcado de núcleo esté activo y configurado:

esxcli system coredump file list

Un resultado similar al siguiente indica que el archivo para el volcado de núcleo está activo y configurado:

```
Path                                              Active Configured Size
------------------------------------------------- ------ ---------- ---------
/vmfs/volumes/52b021c3-.../vmkdump/test.dumpfile True   True       104857600
```

Pasos siguientes

Para obtener información sobre otros comandos que puede usar para administrar los archivos para el volcado de núcleo, consulte la documentación de *Referencia de ESXCLI*.

Desactivar y eliminar un archivo de volcado de núcleo

Desactive un archivo de volcado de núcleo configurado y, si es necesario, quítelo del almacén de datos de VMFS.

Puede desactivar temporalmente el archivo de volcado de núcleo. Si no desea utilizar el archivo desactivado, puede quitarlo del almacén de datos de VMFS. Para quitar el archivo que no se ha desactivado, puede utilizar el comando `esxcli system coredump file remove` con el parámetro `--force | -F`.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 Enumere los archivos de volcado de núcleo:

   esxcli system coredump file list

2 Desactive el archivo de volcado de núcleo con el siguiente comando:

   esxcli system coredump file set --unconfigure | -u

3 Quite el archivo del almacén de datos de VMFS:

   esxcli system coredump file remove --file | -f *file_name*

   El comando admite las siguientes opciones:

Opción	Descripción
--file | -f	Escriba el nombre del archivo de volcado que desea quitar. Si no introduce ningún nombre, el comando quitará el archivo de volcado de núcleo que se configura de forma predeterminada.
--force | -F	Desactive y elimine la configuración del archivo de volcado que se desea quitar. Esta opción se requiere si el archivo aún no se desactivó y sigue activo.

Resultados

El archivo de volcado de núcleo se desactiva y se quita del almacén de datos de VMFS.

Comprobar la coherencia de los metadatos con VOMA

Use vSphere On-disk Metadata Analyzer (VOMA) para identificar y solucionar incidentes de daños de metadatos que afectan los sistemas de archivos o los volúmenes lógicos subyacentes.

Problema

Cuando experimenta problemas con un almacén de datos de VMFS o un recurso flash virtual, puede revisar la consistencia de los metadatos. Por ejemplo, puede realizar una comprobación de metadatos en los siguientes casos:

- Experimenta interrupciones en el almacenamiento.
- Después de volver a construir RAID o realizar un reemplazo de disco.

- Ve errores de metadatos en el archivo `vmkernel.log` similares a los siguientes:

```
cpu11:268057)WARNING: HBX: 599: Volume 50fd60a3-3aae1ae2-3347-0017a4770402
("<Datastore_name>") may be damaged on disk. Corrupt heartbeat detected at offset 3305472:
[HB state 0 offset 6052837899185946624 gen 15439450 stampUS 5 $
```

- No puede tener acceso a archivos en un VMFS.
- Ve que se informa sobre daños para un almacén de datos en las pestañas de eventos de vCenter Server.

Solución

Para comprobar la consistencia de datos, ejecute VOMA en la CLI de un host ESXi. Se puede usar VOMA para comprobar y solucionar problemas menores de inconsistencia de metadatos en un almacén de datos de VMFS o en volúmenes lógicos que respalden el almacén de datos de VMFS.

VOMA puede comprobar y solucionar los siguientes elementos.

Tabla 17-8. Funciones de VOMA

Funciones de VOMA	Descripción
Comprobación y corrección de metadatos	Algunos ejemplos de comprobación y corrección de metadatos son los siguientes: ■ Validación del encabezado de volumen VMFS para mantener la coherencia básica de los metadatos. ■ Comprobación de la coherencia de los archivos de recursos VMFS (archivo de sistema). ■ Comprobación de la ruta de acceso y la conectividad de todos los archivos.
Comprobación de afinidad y corrección de metadatos	Para habilitar la comprobación de afinidad en VMFS6, utilice la opción `-a|--affinityChk`. Varios ejemplos de comprobación y corrección de metadatos de afinidad incluyen lo siguiente: ■ Indicadores de afinidad en tipos de recursos y FS3_ResFileMetadata. ■ Validación de los indicadores de afinidad en metadatos RC de SFB (FS3_ResourceClusterMDVMFS6). ■ Validación de todas las entradas de affinityInfo en rcMeta de RC, incluida la clave de desbordamiento, para asegurarse de que no existen entradas no válidas. Comprobación de entradas faltantes.

Tabla 17-8. Funciones de VOMA (continuación)

Funciones de VOMA	Descripción
Validación de directorio	VOMA puede detectar y corregir los siguientes errores: ■ Daños en el bloque de hash del directorio. ■ Daños en el mapa de asignación. ■ Daños en los bloques de vínculos. ■ Daños en el bloque de entradas de directorio. Según la naturaleza de los daños, VOMA puede corregir solo las entradas dañadas o reconstruir totalmente el bloque de hash, los bloques del mapa de asignación y los bloques de vínculos.
Archivos perdidos y encontrados	Durante una comprobación del sistema de archivos, VOMA puede encontrar los archivos que no tienen referencia en ningún lugar del sistema de archivos. Estos archivos huérfanos son válidos y están completos, pero no tienen una entrada de directorio ni un nombre en el sistema. Si VOMA encuentra archivos huérfanos durante la exploración, crea un directorio denominado lost+found en la raíz del volumen para almacenarlos. Los nombres de los archivos utilizan el formato `Archivo`*`número-de-secuencia`*.

Entre las opciones de comandos que toma la herramienta VOMA se incluyen las siguientes.

Tabla 17-9. Opciones de comandos de VOMA

<table>
<tr><th>Opción de comando</th><th colspan="2">Descripción</th></tr>
<tr><td rowspan="4"><code>-m|--module</code></td><td colspan="2">Los módulos que se ejecutarán incluyen los siguientes:</td></tr>
<tr><td><code>vmfs</code></td><td>Si no se especifica el nombre del módulo, se usa esta opción de manera predeterminada.
Puede comprobar los sistemas de archivos VMFS y los sistemas de archivos que respaldan los recursos flash virtuales. Si especifica este módulo, también se realizan comprobaciones mínimas para LVM.</td></tr>
<tr><td><code>lvm</code></td><td>Compruebe los volúmenes lógicos que respaldan los almacenes de datos de VMFS.</td></tr>
<tr><td><code>ptbl</code></td><td>Comprueba y valida particiones de VMFS, como MBR o GPT.
Si no existe ninguna partición, determina si deberían existir particiones.</td></tr>
<tr><td rowspan="3"><code>-f|--func</code></td><td colspan="2">Las funciones que se realizarán incluyen las siguientes:</td></tr>
<tr><td><code>query</code></td><td>Enumera funciones compatibles con el módulo.</td></tr>
<tr><td><code>check</code></td><td>Comprueba errores.</td></tr>
</table>

Tabla 17-9. Opciones de comandos de VOMA (continuación)

Opción de comando	Descripción	
	`fix`	Comprueba y soluciona errores.
	`dump`	Recopila el volcado de metadatos.
`-a|--affinityChk`	Incluye la comprobación y corrección de afinidades para VMFS6.	
`-d|--device`	Indica el dispositivo o el disco que se va a inspeccionar. Asegúrese de proporcionar la ruta de acceso absoluta hacia la partición del dispositivo que realiza la copia de seguridad del almacén de datos de VMFS. Si el almacén de datos abarca varios dispositivos, proporcione el UUID de la extensión de la cabecera. Por ejemplo, `voma -m vmfs -f check -d /vmfs/devices/disks/naa.xxxx:x` Si utiliza el comando `-x|--extractDump`, introduzca varias rutas de acceso de dispositivo, con un calificador de partición, separadas por comas. La cantidad de rutas de acceso de dispositivos que introduzca es igual a la cantidad de dispositivos abarcados.	
`-b|--blockSize`	Indica el tamaño de bloque de disco.	
`-s|--logfile`	Especifique la ruta de acceso del archivo de registro para la salida de los resultados.	
`-x|--extractDump`	Extrae el volcado recopilado mediante VOMA.	
`-D|--dumpfile`	Indica el archivo de volcado para guardar el volcado de metadatos recopilado.	
`-v|--version`	Muestra la versión de VOMA.	
`-h|--help`	Muestra el mensaje de ayuda para el comando VOMA.	
`-Y`	Indica que ejecuta VOMA sin usar tablas de PE para la resolución de direcciones.	
`-Z| --file`	Indica que ejecuta VOMA en archivos de dispositivos extraídos.	

Ejemplo

Recopila el volcado de metadatos de un volumen abarcado:

voma -m vmfs -f dump -d *head_extent* -D *nombre_archivo_volcado*

Vuelve a extraer el volcado recopilado a los dispositivos de un volumen abarcado:

voma -x *nombre_archivo_volcado* -d *head_extent,extent_2,extent_3...extent_n*

Usar VOMA para comprobar la coherencia de los metadatos

La tarea demuestra cómo usar VOMA para comprobar la coherencia de los metadatos de VMFS. Se puede usar VOMA para comprobar y solucionar problemas menores de inconsistencia de metadatos en un almacén de datos de VMFS o un recurso flash virtual. Ejecute VOMA desde la CLI de un host ESXi.

Requisitos previos

Apague las máquinas virtuales que estén en ejecución o mígrelas a un almacén de datos diferente.

Procedimiento

1 Obtenga el nombre y el número de partición del dispositivo que respalda el almacén de datos de VMFS que quiere revisar.

#esxcli storage vmfs extent list

Las columnas Nombre del dispositivo y Partición en el resultado identifican el dispositivo. Por ejemplo:

```
Volume Name  .....  Device Name                                  Partition
1TB_VMFS6    .....  naa.xxxx                                        3
```

2 Compruebe que no haya errores de VMFS.

Proporciona una ruta de acceso absoluta a la partición del dispositivo que realiza la copia de seguridad del almacén de datos de VMFS, y entregue un número de partición con el nombre del dispositivo. Por ejemplo:

voma -m vmfs -f check -d /vmfs/devices/disks/naa.xxxx:x

El resultado enumera posibles errores. Por ejemplo, el siguiente resultado indica que la dirección de latido no es válida.

```
XXXXXXXXXXXXXXXXXXXXXXX
Phase 2: Checking VMFS heartbeat region
 ON-DISK ERROR: Invalid HB address
Phase 3: Checking all file descriptors.
Phase 4: Checking pathname and connectivity.
Phase 5: Checking resource reference counts.

Total Errors Found:           1
```

Configurar la memoria caché de bloque de puntero de VMFS

Los bloques de puntero, también denominados bloques de direccionamiento indirecto, son los recursos del sistema de archivos que contienen direcciones de bloques de archivos VMFS. Cuando abra un archivo `vmdk` en un host de ESXi, los bloques de punteros relacionados con ese archivo se almacenan en la caché de bloques de punteros. El tamaño de la memoria caché del bloque de puntero es un parámetro configurable.

La memoria caché del bloque de puntero es una memoria caché de todos los hosts que es independiente de VMFS. La memoria caché se comparte entre todos los almacenes de datos a los que se accede desde el mismo host ESXi.

El tamaño de la memoria caché del bloque de puntero se controla mediante `/VMFS3/MinAddressableSpaceTB` y `/VMFS3/MaxAddressableSpaceTB`. Puede configurar los tamaños mínimo y máximo en cada host ESXi.

/VMFS3/MinAddressableSpaceTB

El valor mínimo es la cantidad mínima de memoria que el sistema garantiza para la memoria caché del bloque de puntero. Por ejemplo, 1 TB de espacio de archivo abierto requiere aproximadamente 4 MB de memoria. El valor predeterminado es 10 TB.

/VMFS3/MaxAddressableSpaceTB

El parámetro define el límite máximo de bloques de puntero que pueden almacenarse en la memoria caché. El valor predeterminado es 32 TB. El valor máximo es 128 TB. Por lo general, el valor predeterminado del parámetro `/VMFS3/MaxAddressableSpaceTB` es suficiente.

Sin embargo, a medida que aumenta el tamaño de los archivos vmdk abiertos, también aumenta el número de bloques de puntero relacionados con esos archivos. Si el aumento genera una degradación del rendimiento, puede ajustar el parámetro al valor máximo a fin de proporcionar más espacio para la memoria caché del bloque de puntero. El tamaño máximo de la memoria caché del bloque de puntero se basa en el conjunto de trabajo o los bloques de puntero activos requeridos.

Expulsión de bloque de puntero

El parámetro `/VMFS3/MaxAddressableSpaceTB` también controla el crecimiento de la memoria caché del bloque del puntero. Cuando el tamaño de la memoria caché del bloque de puntero se acerca al tamaño máximo configurado, se inicia el proceso de expulsión del bloque de puntero. El mecanismo deja bloques de puntero activos, pero elimina los bloques no activos o menos activos de la memoria caché para que se pueda reutilizar el espacio.

Puede cambiar los valores de memoria caché del bloque de puntero desde el cuadro de diálogo **Configuración avanzada del sistema** de vSphere Client o el comando `esxcli system settings advanced set -o`.

Puede usar el comando `esxcli storage vmfs pbcache` para obtener información acerca del tamaño de la memoria caché del bloque del puntero y otras estadísticas. Esta información lo ayuda a ajustar los tamaños mínimo y máximo de la memoria caché del bloque del puntero, para que pueda obtener el máximo rendimiento.

Obtener información para la memoria caché de bloque del puntero de VMFS

Puede obtener información sobre el uso de la memoria caché de bloque del puntero de VMFS. Esta información ayuda a comprender cuánto espacio consume la memoria caché de bloque del puntero. También puede identificar si es necesario ajustar los tamaños mínimos y máximos de la memoria caché de bloque del puntero.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

- Para obtener o restablecer las estadísticas de la memoria caché de bloque del puntero, use el siguiente comando:

  `esxcli storage vmfs pbcache`

Opción	Descripción
`get`	Obtener estadísticas de la memoria caché de bloque del puntero de VMFS.
`reset`	Restablecer las estadísticas de la memoria caché de bloque del puntero de VMFS.

Ejemplo: Obtención de estadísticas de la memoria caché de bloque del puntero

```
#esxcli storage vmfs pbcache get
   Cache Capacity Miss Ratio: 0 %
   Cache Size: 0 MiB
   Cache Size Max: 132 MiB
   Cache Usage: 0 %
   Cache Working Set: 0 TiB
   Cache Working Set Max: 32 TiB
   Vmfs Heap Overhead: 0 KiB
   Vmfs Heap Size: 23 MiB
   Vmfs Heap Size Max: 256 MiB
```

Cambiar el tamaño de la memoria caché de bloque del puntero

Puede ajustar los tamaños mínimo y máximo de la memoria caché de bloque del puntero.

Precaución El cambio de opciones avanzadas no se considera un atributo compatible. Por lo general, la configuración predeterminada proporciona resultados óptimos. Cambie las opciones avanzadas solo cuando reciba instrucciones específicas del soporte técnico de VMware, o bien consulte un artículo de la base de conocimientos.

Procedimiento

1. Desplácese hasta el host.
2. Haga clic en la pestaña **Configurar**.
3. En **Sistema**, haga clic en **Configuración avanzada del sistema**.
4. En Configuración avanzada del sistema, seleccione el elemento apropiado.

Opción	Descripción
`VMFS3.MinAddressableSpaceTB`	Tamaño mínimo de todos los archivos abiertos que la memoria caché de VMFS garantiza admitir.
`VMFS3.MaxAddressableSpaceTB`	Tamaño máximo de todos los archivos abiertos que la memoria caché de VMFS admite antes de comenzar la expulsión.

5 Haga clic en el botón **Editar** para modificar el valor.

6 Haga clic en **Aceptar**.

Ejemplo: Utilizar el comando esxcli para cambiar la memoria caché de bloque de puntero

También puede utilizar el comando `esxcli system settings advanced set -o` para modificar el tamaño de la memoria caché de bloque de puntero. En el ejemplo siguiente, se describe cómo establecer el tamaño a su valor máximo de 128 TB.

1 Para cambiar el valor de `/VMFS3/MaxAddressableSpaceTB` a 128 TB, introduzca el siguiente comando:

```
# esxcli system settings advanced set -i 128 -o /VMFS3/
MaxAddressableSpaceTB
```

2 Para confirmar que el valor se estableció correctamente, introduzca este comando:

```
# esxcli system settings advanced list -o /VMFS3/MaxAddressableSpaceTB
```

Descripción de múltiples rutas y conmutación por error

18

Para mantener una conexión constante entre un host y su almacenamiento, ESXi admite múltiples rutas. Con las múltiples rutas, puede utilizar más de una ruta de acceso física que transfiera datos entre el host y un dispositivo de almacenamiento externo.

Si se produce un error en cualquier elemento de la red SAN (como un cable, un conmutador o un adaptador), ESXi puede cambiar a otra ruta de acceso física viable. Este proceso de conmutación de ruta de acceso para evitar componentes con errores se conoce como conmutación por error de ruta de acceso.

Además de la conmutación por error de ruta de acceso, las múltiples rutas proporcionan equilibrio de carga. El equilibrio de carga es el proceso de distribuir las cargas de E/S a través de varias rutas de acceso físicas. El equilibrio de carga reduce o elimina los cuellos de botella potenciales.

Nota La E/S de la máquina virtual podría retrasarse hasta 60 segundos mientras tiene lugar la conmutación por error de la ruta de acceso. Con estos retrasos, la SAN puede estabilizar su configuración después de los cambios de topología. En general, los retrasos de E/S pueden ser más largos en matrices activas-pasivas y más cortos en matrices activas-activas.

Este capítulo incluye los siguientes temas:

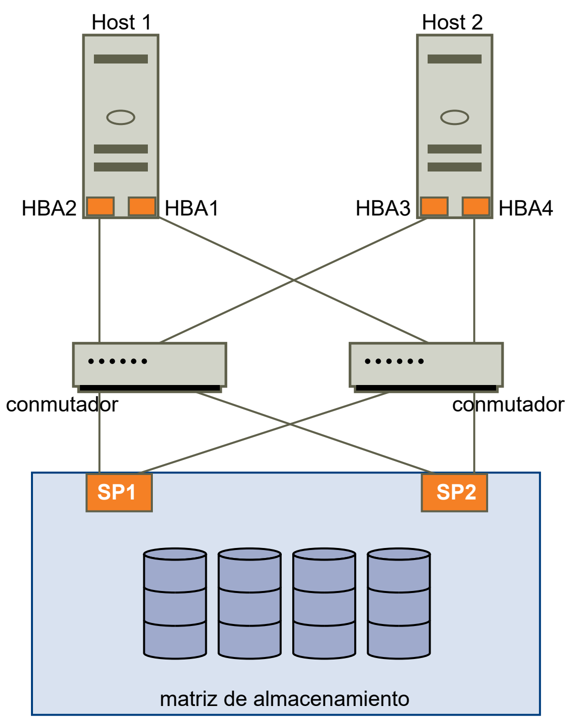
Conmutaciones por error con canal de fibra

Para admitir múltiples rutas, por lo general el host tiene dos o más HBA disponibles. Esta configuración complementa la configuración de múltiples rutas SAN, la cual, por lo general, ofrece

uno o varios conmutadores en el tejido SAN y uno o varios procesadores de almacenamiento en el propio dispositivo de la matriz de almacenamiento.

En la siguiente ilustración, se conectan varias rutas físicas a cada servidor con el dispositivo de almacenamiento. Por ejemplo, si HBA1 o el enlace entre HBA1 y el conmutador de FC genera errores, HBA2 asume el control y permite la conexión. El proceso mediante el cual un HBA asume el control en lugar de otro se denomina conmutación por error HBA.

Figura 18-1. Múltiples rutas y conmutación por error con el canal de fibra



De forma similar, si SP1 genera errores o los vínculos entre SP1 y los conmutadores se interrumpen, SP2 asume el control. SP2 proporciona la conexión entre el conmutador y el dispositivo de almacenamiento. Este proceso se denomina conmutación por error SP. VMware ESXi es compatible con las conmutaciones por error de los HBA y SP.

Conmutación por error basada en host con iSCSI

Cuando configure el host ESXi para múltiples rutas y conmutación por error, podrá usar varios HBA de iSCSI, o combinar varias NIC con el adaptador de iSCSI de software.

Para obtener información sobre los diferentes tipos de adaptadores de iSCSI, consulte Iniciadores iSCSI.

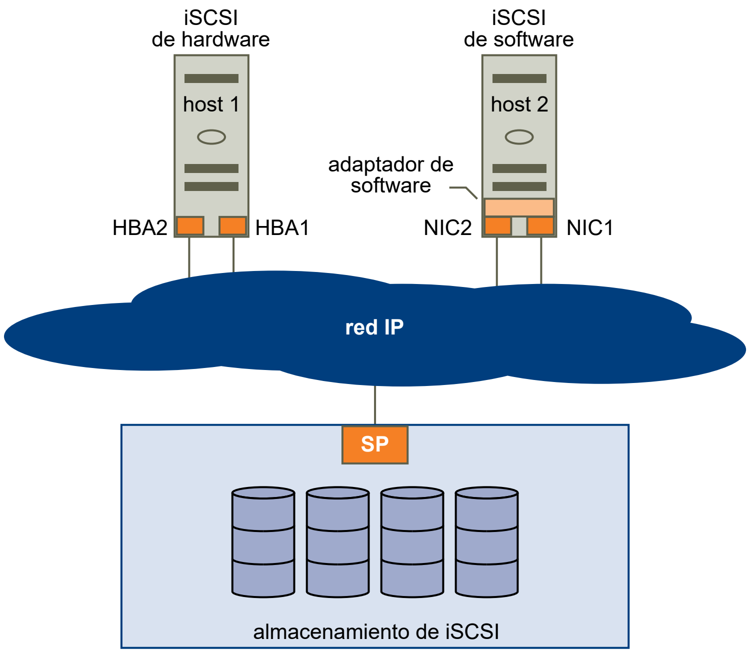
Cuando se utiliza la funcionalidad de múltiples rutas, se aplican consideraciones específicas.

- ESXi no admite múltiples rutas cuando combina un adaptador de hardware independiente con adaptadores de iSCSI de software o de iSCSI dependientes en el mismo host.

- Se admite habilitar múltiples rutas entre adaptadores de software y dependientes en el mismo host.
- En hosts diferentes, se pueden combinar adaptadores dependientes e independientes.

En la siguiente ilustración se muestran opciones de configuración de múltiples rutas posibles con diferentes tipos de iniciadores iSCSI.

Figura 18-2. Conmutar por error de rutas de acceso con base en host



iSCSI de hardware y conmutación por error

Con iSCSI de hardware, el host suele tener dos o más adaptadores de iSCSI de hardware. El host utiliza los adaptadores para comunicarse con el sistema de almacenamiento a través de uno o varios conmutadores. De manera alternativa, la configuración puede incluir un adaptador y dos procesadores de almacenamiento, para que el adaptador pueda utilizar rutas de acceso diferente para comunicarse con el sistema de almacenamiento.

En la ilustración, Host1 tiene dos adaptadores de iSCSI de hardware, HBA1 y HBA2, que ofrecen dos rutas de acceso físicas al sistema de almacenamiento. Los complementos de múltiples rutas del host, ya sean el NMP del VMkernel o cualquier MPP de terceros, tienen acceso a las rutas de forma predeterminada. Los complementos pueden supervisar el estado de las rutas físicas. Si, por ejemplo, HBA1 o el vínculo entre HBA1 y la red generan errores, los complementos de múltiples rutas pueden conmutar la ruta de acceso por HBA2.

iSCSI de software y conmutación por error

Con iSCSI de software, tal como se muestra en el Host 2 de la ilustración, se pueden utilizar varias NIC que proporcionen capacidades de conmutación por error y equilibrio de carga a las conexiones de iSCSI.

Los complementos de múltiples rutas no pueden acceder directamente a las NIC físicas del host. Como resultado, para esta configuración, primero se debe conectar cada NIC física a un puerto VMkernel distinto. A continuación, asocie todos los puertos VMkernel con el iniciador iSCSI de software mediante una técnica de enlace de puertos. Cada puerto VMkernel conectado a una NIC distinta se convierte en una ruta de acceso diferente que pueden utilizar la pila de almacenamiento iSCSI y sus complementos de múltiples rutas con reconocimiento de almacenamiento.

Para obtener información sobre cómo configurar múltiples rutas para iSCSI de software, consulte Configurar la seguridad de red para iSCSI e iSER.

Conmutación por error basada en matrices con iSCSI

Algunos sistemas de almacenamiento iSCSI administran el uso de rutas de acceso de sus puertos de forma automática y transparente para ESXi.

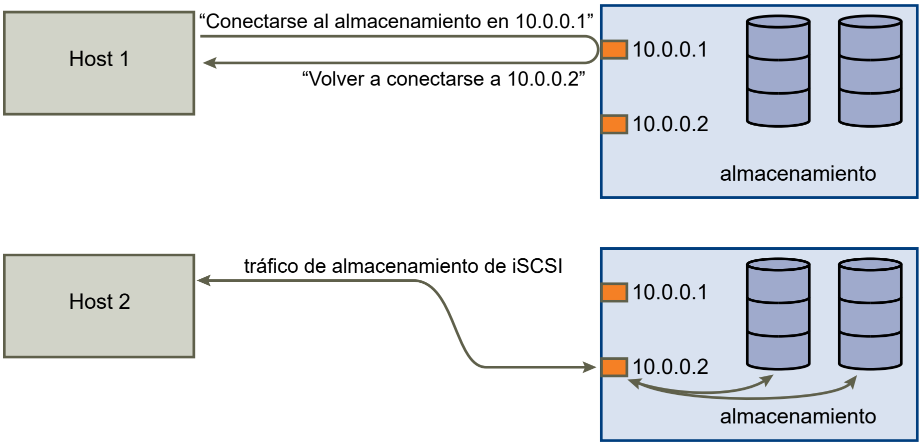
Cuando se utiliza uno de estos sistemas de almacenamiento, el host no ve varios puertos en el almacenamiento y no puede elegir el puerto de almacenamiento al que se conecta. Estos sistemas tienen una sola dirección de puerto virtual que el host utiliza para comunicarse inicialmente. Durante esta comunicación inicial, el sistema de almacenamiento puede redireccionar el host para comunicarse con otro puerto en el sistema de almacenamiento. Los iniciadores iSCSI en el host obedecen a esta solicitud de reconexión y se conectan con un puerto distinto en el sistema. El sistema de almacenamiento utiliza esta técnica para propagar la carga en los puertos disponibles.

Si el host ESXi pierde la conexión con uno de estos puertos, intenta automáticamente reconectarse con el puerto virtual del sistema de almacenamiento, y debería redireccionarse a un puerto activo y utilizable. Esta reconexión y redirección sucede rápidamente, y por lo general no interrumpe las máquinas virtuales en ejecución. Estos sistemas de almacenamiento también pueden solicitar que los iniciadores iSCSI se reconecten al sistema para cambiar el puerto de almacenamiento al que están conectados. Esto permite un uso más eficaz de los diversos puertos.

La ilustración de la redirección de puertos muestra un ejemplo de la redirección de puertos. El host intenta conectarse al puerto virtual 10.0.0.1. El sistema de almacenamiento redirecciona esta solicitud a 10.0.0.2. El host se conecta con 10.0.0.2 y utiliza ese puerto para la comunicación de E/S.

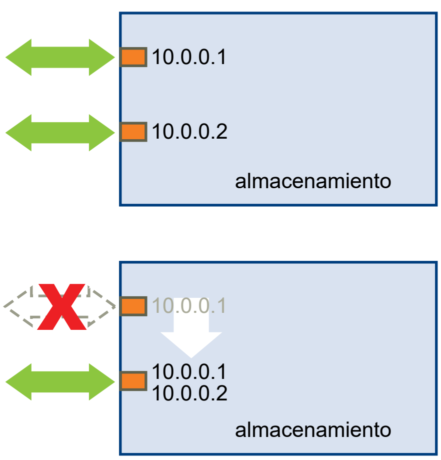
Nota El sistema de almacenamiento no siempre redirecciona las conexiones. El puerto en 10.0.0.1 también podría utilizarse para tráfico.

Figura 18-3. Redirigir puertos



Si el puerto en el sistema de almacenamiento que actúa como puerto virtual deja de estar disponible, el sistema de almacenamiento reasigna la dirección del puerto virtual a otro puerto en el sistema. La reasignación de puertos muestra un ejemplo de este tipo de reasignación. En este caso, el puerto virtual 10.0.0.1 deja de estar disponible y el sistema de almacenamiento reasigna la dirección IP del puerto virtual a un puerto diferente. El segundo puerto responde a ambas direcciones.

Figura 18-4. Reasignar puertos



Con este tipo de conmutación por error basada en matrices, puede tener varias rutas de acceso al almacenamiento solo si utiliza varios puertos en el host ESXi. Estas rutas de acceso son activas-activas. Para obtener información adicional, consulte Administrar sesiones de iSCSI.

Conmutación por error de rutas de acceso y máquinas virtuales

Una conmutación por error de ruta se produce cuando se modifica la ruta activa a un LUN de una ruta a otra. Por lo general, la conmutación por error de ruta se produce como resultado de un error de componente de SAN en la ruta actual.

Cuando una ruta de acceso genera errores, la E/S de almacenamiento puede pausarse durante 30-60 segundos hasta que el host determine que el vínculo no está disponible y realice la conmutación por error. Si intenta mostrar el host, sus dispositivos de almacenamiento o sus adaptadores, es posible que la operación parezca atascarse. Es posible que parezca que las máquinas virtuales con los discos instalados en la SAN no responden. Tras la conmutación por error, E/S reanuda sus actividades normalmente y las máquinas virtuales siguen ejecutándose.

Una máquina virtual de Windows puede interrumpir la E/S y, finalmente, producir un error cuando las conmutaciones por error tardan demasiado. Para evitar un error, configure el valor de tiempo de espera de disco para la máquina virtual de Windows en 60 segundos, como mínimo.

Establecer el tiempo de espera en un sistema operativo invitado Windows

Para evitar interrupciones durante una conmutación por error de una ruta de acceso, aumente el valor de tiempo de espera del disco estándar en un sistema operativo invitado Windows.

Este procedimiento explica cómo cambiar el valor de tiempo de espera con el registro de Windows.

Requisitos previos

Realice una copia de seguridad del registro de Windows.

Procedimiento

1. Seleccione **Inicio > Ejecutar**.
2. Escriba **`regedit.exe`** y haga clic en **Aceptar**.
3. En la vista de jerarquía del panel izquierdo, haga doble clic en **HKEY_LOCAL_MACHINE > Sistema > Conjunto de controles actual > Servicios > Disco**.
4. Haga doble clic en **Valor de tiempo de espera**.
5. Configure los datos de valor a hexadecimal o decimal y haga clic en **Aceptar**.

   Una vez realizado este cambio, Windows espera 60 segundos como mínimo para que finalicen las operaciones de disco demoradas antes de generar errores.
6. Reinicie el sistema operativo invitado para que se aplique el cambio.

Administración de la ruta de acceso y arquitectura de almacenamiento acoplable

En este tema, se presentan los conceptos principales sobre las múltiples rutas de almacenamiento de ESXi.

Arquitectura de almacenamiento acoplable (PSA)

Para administrar múltiples rutas, ESXi utiliza una capa de VMkernel especial, la arquitectura de almacenamiento acoplable (Pluggable Storage Architecture, PSA). PSA es un marco modular

y abierto que coordina diversos módulos de software responsables de las operaciones de múltiples rutas. Estos módulos incluyen los módulos de múltiples rutas genéricos que proporciona VMware: NMP y HPP, y MPP de terceros.

Complemento de múltiples rutas nativo (Native Multipathing Plug-in, NMP)

El NMP es el módulo de múltiples rutas de VMkernel que proporciona ESXi de forma predeterminada. Este módulo asocia rutas de acceso físicas con un dispositivo de almacenamiento específico y proporciona un algoritmo de selección de rutas de acceso predeterminado en función del tipo de matriz. El NMP es extensible y administra submódulos adicionales, denominados directivas de selección de rutas de acceso (Path Selection Policies, PSP) y directivas de tipo de matriz de almacenamiento (Storage Array Type Policies, SATP). Estos submódulos PSP y SATP pueden ser proporcionados por VMware o por un tercero.

Complementos de selección de rutas de acceso (Path Selection Plug-ins, PSP)

Los PSP son submódulos del NMP de VMware. Son los responsables de seleccionar una ruta de acceso física para las solicitudes de E/S.

Complementos de tipo de matriz de almacenamiento (Storage Array Type Plug-ins, SATP)

Los SATP son submódulos del NMP de VMware. Los SATP son los responsables de las operaciones específicas de la matriz. El SATP puede determinar el estado de una ruta de acceso de una matriz específica, realizar una activación de la ruta de acceso y detectar cualquier error en la ruta de acceso.

Complementos de múltiples rutas (Multipathing Plug-ins, MPP)

PSA ofrece una recopilación de API de VMkernel que los terceros pueden utilizar para crear sus propios complementos de múltiples rutas (Multipathing Plug-ins, MPP). Los módulos proporcionan funcionalidades de conmutación por error y equilibrio de carga específicas para una matriz de almacenamiento en particular. Los MPP pueden instalarse en el host ESXi. Pueden ejecutarse en conjunto con los módulos nativos de VMware, o bien reemplazándolos.

Complemento de alto rendimiento (High-Performance Plug-in, HPP) de VMware

El HPP reemplaza al NMP en los dispositivos de alta velocidad, como NVMe. El HPP puede mejorar el rendimiento de los dispositivos flash ultra rápidos que se instalan de forma local en el host ESXi y es el complemento predeterminado que notifica a los destinos de NVMe-oF. Para admitir múltiples rutas, HPP utiliza los esquemas de selección de rutas de acceso (Path Selection Schemes, PSS). Un PSS concreto es responsable de seleccionar las rutas físicas para las solicitudes de E/S.

Para obtener información, consulte Complemento de alto rendimiento de VMware y esquemas de selección de rutas de acceso.

Reglas de notificación

PSA utiliza reglas de notificación para determinar qué complemento posee las rutas de un dispositivo de almacenamiento en particular.

Tabla 18-1. Acrónimos de múltiples rutas

Acrónimo	Definición
PSA	Pluggable Storage Architecture
NMP	Complemento de múltiples rutas nativo. Módulo de múltiples rutas de VMware genérico que utiliza dispositivos de almacenamiento SCSI.
PSP	Complemento de selección de rutas de acceso. Controla la selección de rutas de acceso para un dispositivo de almacenamiento SCSI.
SATP	Complemento de tipo de matriz de almacenamiento. Controla la conmutación por error de rutas de acceso de una matriz de almacenamiento SCSI dada.
MPP (de terceros)	Complemento de múltiples rutas. Un módulo de múltiples rutas desarrollado y proporcionado por un tercero.
HPP	Complemento nativo de alto rendimiento proporcionado por VMware. Se utiliza con dispositivos flash locales y en red ultra rápidos, como NVMe.
PSS	Esquema de selección de rutas de acceso. Controla las múltiples rutas para los dispositivos de almacenamiento NVMe.

Acerca de la arquitectura de almacenamiento acoplable

La arquitectura de almacenamiento acoplable (Pluggable Storage Architecture, PSA) es un marco modular y abierto que coordina los diversos módulos de software responsables de las operaciones de múltiples rutas.

VMware proporciona módulos de múltiples rutas nativos genéricos, denominados NMP y HPP de VMware. Además, PSA ofrece una recopilación de API de VMkernel que pueden utilizar los desarrolladores de terceros. Los desarrolladores de software pueden crear sus propios módulos de equilibrio de carga y conmutación por error para una matriz de almacenamiento en particular. Estos módulos de múltiples rutas (Multipathing Modules, MPP) de terceros se pueden instalar en el host ESXi y pueden ejecutarse además de los módulos nativos de VMware o bien, como sus sustitutos.

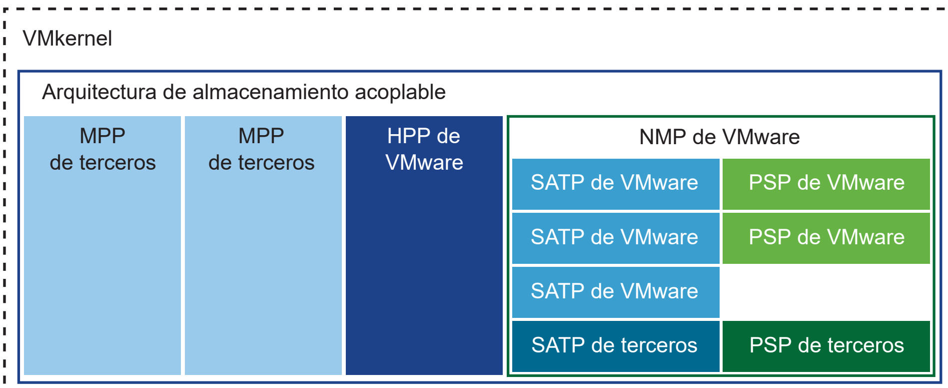
Cuando se coordinan los módulos nativos de VMware y los MPP de terceros instalados, PSA realiza las tareas siguientes:

- Carga y descarga complementos de múltiples rutas.
- Oculta las especificaciones de máquinas virtuales de un complemento en particular.
- Enruta las solicitudes de E/S de un dispositivo lógico específico al MPP que administra ese dispositivo.
- Controla la cola de E/S a los dispositivos lógicos.
- Implementa el uso compartido del ancho de banda de dispositivos lógicos entre máquinas virtuales.
- Controla la cola de E/S a los HBA de almacenamiento físico.
- Controla la detección y eliminación de rutas de acceso físicas.

- Proporciona estadísticas de E/S de rutas de acceso físicas y dispositivos lógicos.

Como se muestra en la ilustración de la arquitectura de almacenamiento acoplable, es posible ejecutar varios MPP de terceros en paralelo con NMP o HPP de VMware. Cuando se instalan, los MPP de terceros pueden reemplazar el comportamiento de los módulos nativos. Los MPP pueden tomar el control de las operaciones de conmutación por error de rutas de acceso y de equilibrio de carga para los dispositivos de almacenamiento especificados.

Figura 18-5. Pluggable Storage Architecture



Complemento de múltiples rutas nativo de VMware

De forma predeterminada, ESXi proporciona un módulo de múltiples rutas extensible denominado complemento de múltiples rutas nativo (NMP).

Por lo general, el NMP de VMware admite todas las matrices de almacenamiento enumeradas en el HCL de almacenamiento de VMware y proporciona un algoritmo de selección de rutas de acceso predeterminado en función del tipo de matriz. El NMP asocia un conjunto de rutas de acceso físicas con un dispositivo de almacenamiento específico, o LUN.

Para otras operaciones de múltiples rutas, NMP utiliza submódulos denominados SATP y PSP. NMP delega en SATP los detalles específicos del control de la conmutación por error de la ruta de acceso del dispositivo. El submódulo PSP controla la selección de rutas de acceso del dispositivo.

Por lo general, NMP realiza las siguientes operaciones:

- Administra las notificaciones y la anulación de notificaciones de una ruta de acceso física.
- Registra y anula el registro de dispositivos lógicos.
- Asocia rutas de acceso físicas con dispositivos lógicos.
- Admite la detección y la corrección de errores de rutas de acceso.
- Procesa solicitudes de E/S en dispositivos lógicos:
  - Selecciona una ruta de acceso física óptima para la solicitud.
  - Realiza las acciones necesarias para controlar los errores de ruta de acceso y los reintentos de comandos de E/S.

- Admite tareas de administración, como el restablecimiento de dispositivos lógicos.

ESXi automáticamente instala un submódulo SATP adecuado para la matriz utilizada. No es necesario que obtenga o descargue ningún SATP.

Flujo NMP de E/S de VMware

Cuando una máquina virtual emite una solicitud de E/S a un dispositivo de almacenamiento administrado por el NMP, se lleva a cabo el proceso siguiente.

1 El NMP llama al PSP asignado a este dispositivo de almacenamiento.
2 El PSP selecciona una ruta de acceso física adecuada en la cual se pueda emitir la E/S.
3 El NMP emite la solicitud de E/S en la ruta de acceso seleccionada por el PSP.
4 Si la operación de E/S se realiza correctamente, el NMP informa la finalización.
5 De lo contrario, el NMP llama al SATP adecuado.
6 El SATP interpreta los errores de comando de E/S y, cuando corresponde, activa las rutas de acceso inactivas.
7 Se le pide al PSP que seleccione la nueva ruta de acceso en la cual se pueda emitir la E/S.

Mostrar módulos de múltiples rutas

Use el comando `esxcli` para enumerar todos los módulos de múltiples rutas cargados en el sistema. Los módulos de múltiples rutas administran las rutas de acceso físicas que conectan el host con el almacenamiento. Los módulos incluyen HPP y NMP nativo de VMware, y cualquier MPP de terceros.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

◆ Para enumerar los módulos de múltiples rutas, ejecute el siguiente comando:

`esxcli storage core plugin list --plugin-class=MP`

Resultados

Este comando generalmente muestra el módulo NMP y, si están cargados, los módulos HPP y MASK_PATH. También se muestran los módulos MPP de terceros en el caso de que se hayan cargado.

```
Plugin name  Plugin class
-----------  ------------
NMP          MP
```

Para obtener más información sobre el comando, consulte la documentación de *Conceptos y ejemplos de ESXCLI* y *Referencia de ESXCLI*.

Mostrar dispositivos de almacenamiento NMP

Use el comando `esxcli` para enumerar todos los dispositivos de almacenamiento que controla VMware NMP y mostrar información de SATP y PSP asociada con cada dispositivo.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

- Para enumerar todos los dispositivos de almacenamiento, ejecute el comando siguiente:

  `esxcli storage nmp device list`

  Utilice el parámetro **`--device | -d=`*`device_ID`*** para filtrar los resultados de este comando de modo que muestren un solo dispositivo.

Ejemplo: Mostrar dispositivos de almacenamiento NMP

```
# esxcli storage nmp device list
mpx.vmhba1:C0:T2:L0
   Device Display Name: Local VMware Disk (mpx.vmhba1:C0:T2:L0)
   Storage Array Type: VMW_SATP_LOCAL
   Storage Array Type Device Config: SATP VMW_SATP_LOCAL does not support device
configuration.
   Path Selection Policy: VMW_PSP_FIXED
   Path Selection Policy Device Config: {preferred=vmhba1:C0:T2:L0;current=vmhba1:C0:T2:L0}
   Path Selection Policy Device Custom Config:
   Working Paths: vmhba1:C0:T2:L0
   Is USB: false

......

eui.6238666462643332
   Device Display Name: SCST_BIO iSCSI Disk (eui.6238666462643332)
   Storage Array Type: VMW_SATP_DEFAULT_AA
   Storage Array Type Device Config: {action_OnRetryErrors=off}
   Path Selection Policy: VMW_PSP_FIXED
   Path Selection Policy Device Config: {preferred=vmhba65:C0:T0:L0;current=vmhba65:C0:T0:L0}
   Path Selection Policy Device Custom Config:
   Working Paths: vmhba65:C0:T0:L0
   Is USB: false
```

Para obtener más información sobre el comando, consulte la documentación de *Conceptos y ejemplos de ESXCLI* y *Referencia de ESXCLI*.

Directivas y complementos de selección de rutas de acceso

Los complementos de selección de rutas de acceso (Path Selection Plug-ins, PSP) de VMware son responsables de la selección de una ruta de acceso física para las solicitudes de E/S.

Los complementos son submódulos del NMP de VMware. NMP asigna un submódulo PSP predeterminado para cada dispositivo lógico según el tipo de dispositivo. Es posible anular la PSP predeterminada. Para obtener más información, consulte Cambiar la directiva de selección de rutas de acceso.

Cada PSP habilita y aplica una directiva de selección de rutas de acceso correspondiente.

VMW_PSP_MRU: Utilizados más recientemente (VMware)

VMW_PSP_MRU aplica la directiva Utilizada recientemente (VMware). Selecciona la primera ruta de acceso en funcionamiento detectada en el momento del arranque del sistema. Cuando la ruta de acceso deja de estar disponible, el host selecciona una ruta de acceso alternativa. El host no se revierte a la ruta de acceso original cuando esa ruta pasa a estar disponible. La directiva Utilizada recientemente no incluye la configuración de ruta de acceso preferida. Esta directiva es la predeterminada para la mayoría de los dispositivos de almacenamiento activo-pasivo.

VMW_PSP_MRU es compatible con la clasificación de rutas de acceso. Para establecer clasificaciones a rutas de acceso individuales, utilice el comando `esxcli storage nmp psp generic pathconfig set`. Para obtener más información, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2003468 y la documentación de *Referencia de ESXCLI*.

VMW_PSP_FIXED: Fija (VMware)

VMW_PSP_FIXED implementa esta directiva Fija (VMware). La directiva utiliza la ruta de acceso preferida designada. Si no se asigna la ruta de acceso preferida, la directiva selecciona la primera ruta de acceso en funcionamiento detectada en el momento del arranque del sistema. Si la ruta de acceso preferida deja de estar disponible, el host selecciona una ruta alternativa disponible. El host regresa a la ruta de acceso preferida definida previamente cuando vuelve a estar disponible.

La directiva fija es la predeterminada para la mayoría de los dispositivos de almacenamiento activos-activos.

VMW_PSP_RR: Round Robin (VMware)

VMW_PSP_RR habilita la directiva Round Robin (VMware). Round Robin es la directiva predeterminada de muchas matrices. Utiliza un algoritmo de selección de rutas de acceso automático que rota a través de las rutas de acceso configuradas.

Las matrices activas-activas y activas-pasivas usan la directiva para implementar el equilibrio de carga entre las rutas de acceso para diferentes LUN. Con las matrices activas-pasivas, la directiva utiliza rutas de acceso activas. Con las matrices activas-activas, la directiva utiliza las rutas de acceso disponibles.

El mecanismo de latencia que se activa para la directiva de forma predeterminada permite una mayor capacidad de adaptación. Para conseguir mejores resultados de equilibrio de carga, el

mecanismo selecciona de forma dinámica una ruta de acceso óptima teniendo en cuenta las siguientes características de la ruta de acceso:

- Ancho de banda de E/S
- Latencia de ruta de acceso

Para cambiar los parámetros predeterminados de la directiva Round Robin de latencia adaptable o para deshabilitar el mecanismo de latencia, consulte Cambiar los parámetros predeterminados de una latencia de Round Robin.

Para establecer otros parámetros configurables para VMW_PSP_RR, utilice el comando `esxcli storage nmp psp roundrobin`. Para obtener información detallada, consulte la documentación de *Referencia de ESXCLI*.

SATP de VMware

Los complementos de tipo de matriz de almacenamiento (Storage Array Type Plug-in, SATP) son responsables de las operaciones específicas de la matriz. Los SATP son submódulos del NMP de VMware.

ESXi ofrece un SATP por cada tipo de matriz que VMware admite. ESXi también proporciona SATP predeterminados que admiten dispositivos no específicos de tipo activo-activo, activo-pasivo, ALUA y local.

Cada SATP admite características especiales de un cierto tipo de matriz de almacenamiento. El SATP puede realizar las operaciones específicas de la matriz necesarias para detectar el estado de la ruta y activar una ruta inactiva. Como resultado, el módulo NMP mismo puede funcionar con varias matrices de almacenamiento sin tener que estar pendiente de las especificaciones del dispositivo de almacenamiento.

Por lo general, NMP determina el SATP que se utilizará para un dispositivo de almacenamiento específico y asocia el SATP con las rutas físicas de ese dispositivo de almacenamiento. El SATP implementa tareas entre las que se incluyen las siguientes:

- Supervisa el estado de cada ruta de acceso física.
- Informa los cambios de estado de cada ruta de acceso física.
- Realiza acciones específicas de matriz necesarias para la conmutación por error del almacenamiento. Por ejemplo, en el caso de dispositivos activo-pasivos, puede activar las rutas de acceso pasivas.

ESXi incluye varios módulos de SATP genéricos para matrices de almacenamiento.

VMW_SATP_LOCAL

El SATP para dispositivos locales de conexión directa.

A partir de vSphere 6.5 Update 2, VMW_SATP_LOCAL ofrece compatibilidad con múltiples rutas para los dispositivos locales, salvo para los dispositivos en formato nativo 4K. A diferencia de lo que se requería en versiones anteriores de vSphere, ya no es necesario utilizar otros SATP para reclamar múltiples rutas a los dispositivos locales.

VMW_SATP_LOCAL es compatible con los complementos de selección de rutas VMW_PSP_MRU y VMW_PSP_FIXED, pero es incompatible con VMW_PSP_RR.

VMW_SATP_DEFAULT_AA

El SATP genérico para matrices de tipo activo-activo.

VMW_SATP_DEFAULT_AP

El SATP genérico para matrices de tipo activo-pasivo.

VMW_SATP_ALUA

El SATP para matrices compatibles con ALUA.

Para obtener más información, consulte la *Guía de compatibilidad de VMware* y la documentación de *Referencia de ESXCLI*.

Mostrar SATP para el host

Use el comando `esxcli` para enumerar los SATP de NMP de VMware cargados en el sistema. Muestre información sobre los SATP.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

- Para enumerar los SATP de VMware, ejecute el comando siguiente:

  `esxcli storage nmp satp list`

Resultados

Para cada SATP, el resultado muestra el tipo de sistema o matriz de almacenamiento que admite el SATP, y el PSP predeterminado de cualquier LUN que use este SATP. `Placeholder (plugin not loaded)` en la columna Descripción indica que el SATP no se cargó.

Ejemplo: Mostrar SATP para el host

```
# esxcli storage nmp satp list
Name                 Default PSP    Description
VMW_SATP_MSA         VMW_PSP_MRU    Placeholder (plugin not loaded)
VMW_SATP_ALUA        VMW_PSP_MRU    Placeholder (plugin not loaded)
VMW_SATP_DEFAULT_AP  VMW_PSP_MRU    Placeholder (plugin not loaded)
VMW_SATP_SVC         VMW_PSP_FIXED  Placeholder (plugin not loaded)
VMW_SATP_EQL         VMW_PSP_FIXED  Placeholder (plugin not loaded)
VMW_SATP_INV         VMW_PSP_FIXED  Placeholder (plugin not loaded)
VMW_SATP_EVA         VMW_PSP_FIXED  Placeholder (plugin not loaded)
VMW_SATP_ALUA_CX     VMW_PSP_RR     Placeholder (plugin not loaded)
VMW_SATP_SYMM        VMW_PSP_RR     Placeholder (plugin not loaded)
```

```
VMW_SATP_CX          VMW_PSP_MRU    Placeholder (plugin not loaded)
VMW_SATP_LSI         VMW_PSP_MRU    Placeholder (plugin not loaded)
VMW_SATP_DEFAULT_AA  VMW_PSP_FIXED  Supports non-specific active/active arrays
VMW_SATP_LOCAL       VMW_PSP_FIXED  Supports direct attached devices
```

Para obtener más información sobre el comando, consulte la documentación de *Conceptos y ejemplos de ESXCLI* y *Referencia de ESXCLI*.

Complemento de alto rendimiento de VMware y esquemas de selección de rutas de acceso

VMware proporciona el complemento de alto rendimiento (High-Performance Plug-in, HPP) para mejorar el rendimiento de dispositivos de almacenamiento en el host ESXi.

HPP reemplaza a NMP en los dispositivos de alta velocidad, como NVMe. El HPP es el complemento predeterminado que notifica los destinos de NVMe-oF. Dentro de ESXi, se emulan los destinos NVMe-oF, y se presentan a los usuarios como destinos SCSI. HPP solo admite destinos de ALUA implícitos y activos/activos.

En vSphere 7.0 Update 1 y versiones anteriores, NMP sigue siendo el complemento predeterminado para los dispositivos NVMe locales, pero puede reemplazarlo por HPP. A partir de vSphere 7.0 Update 2, HPP se convierte en el complemento predeterminado para los dispositivos NVMe y SCSI locales, pero puede reemplazarlo por NMP.

Compatibilidad con HPP	vSphere 7.0 Update 1	vSphere 7.0 Update 2 y Update 3
Dispositivos de almacenamiento	PCIe NVMe local NVMe-oF compartido (solo destinos de ALUA activos/activos y de ALUA implícitos)	NVMe y SCSI locales NVMe-oF compartido (solo destinos de ALUA activos/activos y de ALUA implícitos)
Múltiples rutas	Sí	Sí
Complementos de segundo nivel	No Esquemas de selección de rutas de acceso (PSS)	No
Reservas persistentes de SCSI-3	No	No
Dispositivos 4Kn con emulación de software	No	Sí

Esquemas de selección de rutas de acceso

Para admitir múltiples rutas, HPP utiliza los esquemas de selección de rutas de acceso (PSS) al seleccionar rutas de acceso físicas para las solicitudes de E/S.

Puede utilizar vSphere Client o el comando `esxcli` para cambiar el mecanismo de selección de rutas de acceso predeterminado.

Para obtener información sobre cómo configurar los mecanismos de ruta de acceso en vSphere Client, consulte Cambiar la directiva de selección de rutas de acceso. Para configurar con el comando `esxcli`, consulte Comandos ESXCLI HPP de ESXi.

ESXi admite los siguientes mecanismos de selección de rutas de acceso.

FIJA

Con este esquema, se utiliza una ruta de acceso preferida designada para las solicitudes de E/S. Si la ruta de acceso preferida no está asignada, el host selecciona la primera ruta de acceso en funcionamiento detectada en el momento del arranque del sistema. Si la ruta de acceso preferida deja de estar disponible, el host selecciona una ruta alternativa disponible. El host regresa a la ruta de acceso preferida definida previamente cuando vuelve a estar disponible.

Cuando configure **FIJO** como mecanismo de selección de rutas de acceso, seleccione la ruta de acceso preferida.

LB-RR (equilibrio de carga - Round Robin)

Este es el esquema predeterminado para los dispositivos reclamados por HPP. Después de transferir un número especificado de bytes o E/S en una ruta de acceso actual, el esquema selecciona la ruta de acceso mediante el algoritmo Round Robin.

Para configurar el mecanismo de selección de rutas de acceso de **LB-RR**, especifique las siguientes propiedades:

- **IOPS** indica el recuento de E/S en la ruta de acceso que se utilizará como criterio para cambiar una ruta de acceso para el dispositivo.
- **Bytes** indica el recuento de bytes en la ruta de acceso que se utilizará como criterio para cambiar una ruta de acceso para el dispositivo.

LB-IOPS (equilibrio de carga - IOPS)

Después de transferir un número especificado de E/S en una ruta de acceso actual, el valor predeterminado es 1000, el sistema selecciona una ruta de acceso óptima que tenga el menor número de E/S pendientes.

Al configurar este mecanismo, especifique el parámetro **IOPS** para indicar el recuento de E/S en la ruta de acceso que se utilizará como criterio para cambiar una ruta de acceso para el dispositivo.

LB-BYTES (equilibrio de carga - bytes)

Después de transferir un número especificado de bytes en una ruta de acceso actual, el valor predeterminado es 10 MB, el sistema selecciona una ruta de acceso óptima que tiene el menor número de bytes pendientes.

Para configurar este mecanismo, utilice el parámetro **Bytes** para indicar el recuento de bytes en la ruta de acceso que se utilizará como criterio para cambiar una ruta de acceso para el dispositivo.

Equilibrio de carga-latencia (LB - latencia)

Para conseguir mejores resultados de equilibrio de carga, el mecanismo selecciona de forma dinámica una ruta de acceso óptima teniendo en cuenta las siguientes características de la ruta de acceso:

- El parámetro **Tiempo de evaluación de latencia** indica en qué intervalo de tiempo, en milisegundos, se debe evaluar la latencia de las rutas de acceso.
- El parámetro **E/S de muestreo por ruta de acceso** controla cuántas operaciones de E/S de ejemplo se deben emitir en cada ruta de acceso para calcular la latencia de la ruta de acceso.

Prácticas recomendadas de HPP

Para alcanzar el rendimiento más rápido desde un dispositivo de almacenamiento de alta velocidad, siga estas recomendaciones.

- Utilice la versión de vSphere que admita HPP.
- Utilice HPP para los dispositivos NVMe y SCSI locales, y dispositivos NVMe-oF.
- Si utiliza dispositivos NVMe over Fibre Channel, siga las recomendaciones generales para el almacenamiento de Fibre Channel. Consulte Capítulo 4 Usar ESXi con SAN de canal de fibra.
- Si usa NVMe-oF, no mezcle los tipos de transporte para acceder al mismo espacio de nombres.
- Cuando utilice espacios de nombres NVMe-oF, asegúrese de que se presenten rutas activas al host. Los espacios de nombres no se pueden registrar hasta que se detecte la ruta de acceso activa.
- Configure las máquinas virtuales para que usen las controladoras VMware Paravirtual. Consulte la documentación de *Administrar máquinas virtuales de vSphere*.
- Establezca el umbral de sensibilidad de latencia.
- Si una sola máquina virtual impulsa una parte significativa de la carga de trabajo de E/S del dispositivo, considere la posibilidad de distribuir las operaciones de E/S entre varios discos virtuales. Asocie los discos a distintas controladoras virtuales en la máquina virtual.

  De lo contrario, el rendimiento de las operaciones de E/S podría verse limitado por la saturación del núcleo de CPU que se encarga de procesar las operaciones de E/S en una controladora de almacenamiento virtual en particular.

Para obtener información sobre identificadores de dispositivos para dispositivos NVMe que solo admiten el formato NGUID, consulte Dispositivos NVMe con identificadores de dispositivo NGUID.

Habilitar el complemento de alto rendimiento y los esquemas de selección de rutas de acceso

El complemento de alto rendimiento (HPP) es el complemento predeterminado que reclama dispositivos NVMe y SCSI locales, y destinos NVMe-oF. Si es necesario, puede reemplazarlo por NMP. En vSphere versión 7.0 Update 1 y versiones anteriores, NMP sigue siendo el complemento predeterminado para dispositivos NVMe y SCSI locales, pero puede reemplazarlo por HPP.

Use el comando `esxcli storage core claimrule add` para habilitar HPP o NMP en el host ESXi.

Para ejecutar `esxcli storage core claimrule add`, puede usar ESXi Shell o vSphere CLI. Para obtener más información, consulte *Introducción a ESXCLI* y *Referencia de ESXCLI*.

Los ejemplos de este tema muestran cómo habilitar HPP y configurar los esquemas de selección de rutas de acceso (Path Selection Schemes, PSS).

Nota No se admite la habilitación de HPP en hosts ESXi con arranque PXE.

Requisitos previos

Configure el entorno de almacenamiento de NVMe de VMware. Para obtener más información, consulte Capítulo 16 Acerca del almacenamiento de NVMe de VMware.

Procedimiento

1 Cree una regla de notificación de HPP mediante la ejecución del comando `esxcli storage core claimrule add`.

   Utilice uno de los siguientes métodos para agregar la regla de notificación:

Método	Descripción
Según el modelo de controlador de NVMe	**`esxcli storage core claimrule add --type vendor --nvme-controller-model`** Por ejemplo, **`esxcli storage core claimrule add --rule 429 --type vendor --nvme-controller-model "ABCD*" --plugin HPP`**
Según el ID de proveedor y de subproveedor de PCI	**`esxcli storage core claimrule add --type vendor --pci-vendor-id --pci-sub-vendor-id`** Por ejemplo, **`esxcli storage core claimrule add --rule 429 --type vendor --pci-vendor-id 8086 --pci-sub-vendor-id 8086 --plugin HPP`**.

2 Configure el PSS.

   Utilice uno de los siguientes métodos.

Método	Descripción
Configure el PSS en función del ID de dispositivo	**`esxcli storage hpp device set`** Por ejemplo, **`esxcli storage hpp device set --device=`*`device`*` --pss=FIXED --path=preferred path`**
Configure el PSS en función del proveedor/modelo	Utilice la opción **`--config-string`** con el comando **`esxcli storage core claimrule add`**. Por ejemplo, **`esxcli storage core claimrule add -r 914 -t vendor -V `*`vendor`*` -M `*`model`*` -P HPP --config-string "pss=LB-Latency,latency-eval-time=40000"`**

3 Reinicie el host para que se apliquen los cambios.

Establecer el umbral de sensibilidad de latencia

Cuando utilice HPP para los dispositivos de almacenamiento, establezca el umbral de sensibilidad de latencia del dispositivo para que las operaciones de E/S puedan evitar al programador de E/S.

De forma predeterminada, ESXi pasa cada E/S mediante el programador de E/S. El uso del programador, sin embargo, podría crear una cola interna, lo cual no es eficaz con los dispositivos de almacenamiento de alta velocidad.

Puede configurar el umbral de sensibilidad de latencia y habilitar el mecanismo de envío directo que ayuda a las operaciones de E/S a omitir al programador. Con este mecanismo habilitado, las operaciones de E/S pasan directamente desde PSA, a través de HPP, hacia el controlador del dispositivo.

Para que el envío directo funcione correctamente, la latencia promedio de E/S observada debe ser menor que el umbral de latencia especificado. Si la latencia de E/S supera el umbral de latencia, el sistema detiene el envío directo y vuelve a utilizar temporalmente el programador de E/S. Cuando la latencia promedio de E/S vuelve a caer por debajo del umbral de latencia, se reanuda el envío directo.

Puede establecer el umbral de latencia de una familia de dispositivos reclamados por HPP. Establezca el umbral de latencia mediante el par de proveedor y modelo, el modelo de controladora o el par ID de proveedor PCIe y ID de subproveedor.

Procedimiento

1 Establezca el umbral de sensibilidad de latencia para el dispositivo con el siguiente comando:

   Valor **`esxcli Storage Core Device LatencyThreshold Set-t`** ***`en milisegundos`***

   Use una de las siguientes opciones.

Opción	Ejemplo
Proveedor/modelo	Establezca el parámetro de umbral sensible de latencia para todos los dispositivos con el proveedor y el modelo indicados: **`esxcli Storage Core Device LatencyThreshold Set-v ' vendor1 '-m ' Model1 '-t 10`**
Modelo de controlador NVMe	Establezca el umbral sensible de latencia para todos los dispositivos NVMe con el modelo de controlador indicado: **`esxcli Storage Core Device LatencyThreshold Set-c ' controller_model1 '-t 10`**
ID de proveedor/subproveedor de PCIe	Establezca el umbral de sensibilidad de latencia para los dispositivos con 0x8086 como identificador de proveedor de PCIe y 0x8086 como identificador de subproveedor de PCIe. **`esxcli Storage Core Device LatencyThreshold Set-p ' 8086 '-s ' 8086 '-t 10`**

2 Compruebe que el umbral de latencia esté establecido:

esxcli storage core device latencythreshold list

```
Device                Latency Sensitive Threshold
--------------------  ---------------------------
naa.55cd2e404c1728aa               0 milliseconds
naa.500056b34036cdfd               0 milliseconds
naa.55cd2e404c172bd6              50 milliseconds
```

3 Supervise el estado del umbral de sensibilidad de latencia. Compruebe los registros de VMkernel para las siguientes entradas:

- `Latency Sensitive Gatekeeper turned on for device` *device*`. Threshold of` *XX* `msec is larger than max completion time of` *YYY* `msec`
- `Latency Sensitive Gatekeeper turned off for device` *device*`. Threshold of` *XX* `msec is exceeded by command completed in` *YYY* `msec`

Comandos ESXCLI HPP de ESXi

Puede utilizar los comandos CLI de vSphere o ESXi Shell para configurar y supervisar el complemento de alto rendimiento.

Consulte *Introducción a ESXCLI* para obtener una introducción y *Referencia de ESXCLI* para conocer los detalles sobre el uso del comando `esxcli`.

Comando	Descripción	Opciones
`esxcli storage hpp path list`	Enumerar las rutas de acceso actualmente reclamadas por el complemento de alto rendimiento.	`-d|--device=`*device* Muestre la información de un dispositivo específico. `-p|--path=`*path* Limite la salida a una ruta de acceso específica.
`esxcli storage hpp device list`	Enumerar los dispositivos actualmente controlados por el complemento de alto rendimiento.	`-d|--device=`*device* Muestre un dispositivo específico.

Comando	Descripción	Opciones
`esxcli storage hpp device set`	Configurar los ajustes de un dispositivo HPP.	`-B|--bytes=`*`long`* Bytes máximos en la ruta de acceso, después del cual se cambia la ruta de acceso. `--cfg-file` Actualice el tiempo de ejecución y el archivo de configuración con la nueva configuración. Si otro PSS reclama el dispositivo, ignore cualquier error cuando se aplique a la configuración de tiempo de ejecución. `-d|--device=`*`device`* El dispositivo HPP donde se opera. Utilizar cualquiera de los UID que informa el dispositivo. Requerido. `-I|--iops=` *`long`* IOPS máximos en la ruta de acceso, después de los cuales se cambia la ruta de acceso. `-T|--latency-eval-time=` *`long`* Controle en qué intervalo, en milisegundo, se debe evaluar la latencia de las rutas de acceso. `-L|--mark-device-local=` *`bool`* Establezca HPP para tratar el dispositivo como local o no. `-M|--mark-device-ssd=`*`bool`* Especifique si HPP trata al dispositivo como un disco SSD. `-p|--path=` *`str`* La ruta de acceso que se va a establecer como la ruta de acceso preferida para el dispositivo. `-P|--pss=` *`pss_name`* El esquema de selección de rutas de acceso que se asignará al dispositivo. Si no especifica el valor, el sistema selecciona el valor predeterminado. Para obtener la descripción de los esquemas de selección de rutas de acceso, consulte Complemento de alto rendimiento de VMware y esquemas de selección de rutas de acceso. Las opciones incluyen: ■ **`FIJO`** Utilice la subopción `-p|--path=`*`str`* para establecer la ruta de acceso preferida. ■ **`LB-Bytes`** Utilice la subopción `-B|--bytes=` *`long`* para especificar la entrada. ■ **`LB-IOPs`** Utilice la subopción `-I|--iops=` *`long`* para especificar la entrada. ■ **`LB-Latency`** Las subopciones incluyen: `-T|--latency-eval-time=`*`long`*

Comando	Descripción	Opciones

		`-S|--sampling-ios-per-path=long`
		■ **LB-RR** Predeterminado
		Las subopciones incluyen:
		`-B|--bytes=long`
		`-I|--iops=long`
		`-S|--sampling-ios-per-path= long` Controle cuántas operaciones de E/S de ejemplo se deben emitir en cada ruta de acceso para calcular la latencia de la ruta de acceso.
		`-U|--use-ano= bool` Establezca la opción en `true` para incluir rutas de acceso no optimizadas en el conjunto de rutas de acceso activas utilizadas para emitir operaciones de E/S en este dispositivo. De lo contrario, establezca la opción en `false`.

`esxcli storage hpp device usermarkedssd list`	Enumerar los dispositivos que el usuario marcó o desmarcó como SSD.	`-d|--device=device` Limite la salida a un dispositivo específico.

Ver y administrar rutas de acceso

Cuando inicia el host ESXi o vuelve a examinar el adaptador de almacenamiento, el host detecta todas las rutas de acceso físicas hacia los dispositivos de almacenamiento disponibles para el host. BA partir de un conjunto de reglas de notificación, el host determina qué módulo de múltiples rutas (NMP, HPP o MPP) posee las rutas de acceso a un dispositivo determinado.

El módulo que posee el dispositivo se convierte en el responsable de administrar el soporte de múltiples rutas del dispositivo. De forma predeterminada, el host realiza una evaluación periódica de la ruta de acceso cada cinco minutos y asigna las rutas de acceso sin notificar al módulo correspondiente.

Para las rutas de acceso administradas por el módulo de NMP, se usa un segundo conjunto de reglas de notificación. Estas reglas asignan módulos de SATP y PSP a cada dispositivo de almacenamiento y determinan qué directiva de tipo de matriz de almacenamiento y qué directiva de selección de ruta de acceso se aplicarán.

Utilice vSphere Client para ver la directiva de tipo de matriz de almacenamiento y la directiva de selección de rutas de acceso asignadas a un dispositivo de almacenamiento específico. También puede comprobar el estado de todas las rutas de acceso disponibles para este dispositivo de almacenamiento. Si es necesario, puede cambiar la directiva de selección de rutas de acceso predeterminada a través del cliente.

Para cambiar el módulo de múltiples rutas predeterminado o el módulo SATP, modifique las reglas de notificación mediante vSphere CLI.

Puede encontrar información sobre la modificación de las reglas de notificación en Usar reglas de notificación.

Ver rutas de acceso de dispositivos de almacenamiento

Visualice las directivas de múltiples rutas que utiliza el host para un dispositivo de almacenamiento específico y el estado de todas las rutas de acceso disponibles para este dispositivo de almacenamiento.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Dispositivos de almacenamiento**.

4 Seleccione el dispositivo de almacenamiento cuyas rutas de acceso desea ver.

5 Haga clic en la pestaña **Propiedades** y revise el módulo que posee el dispositivo, por ejemplo, NMP o HPP.

   En Directivas de múltiples rutas, también puede ver la directiva de selección de ruta de acceso y, si corresponde, la directiva de tipo de matriz de almacenamiento asignada al dispositivo.

6 Haga clic en la pestaña **Rutas de acceso** para revisar todas las rutas de acceso disponibles para el dispositivo de almacenamiento y el estado de cada ruta de acceso. Puede aparecer la siguiente información sobre el estado de la ruta de acceso:

Estado	Descripción
Activo (E/S)	Ruta de trabajo o múltiples rutas de acceso que actualmente transfieren datos.
En espera	Rutas de acceso inactivas. Si se produce un error en la ruta activa, pueden entrar en funcionamiento y comenzar a transferir E/S.
Deshabilitado	Rutas de acceso deshabilitadas por el administrador.
Inactiva	Rutas de acceso que ya no están disponibles para el procesamiento de E/S. Un error en un medio físico o la configuración incorrecta de una matriz pueden provocar este estado.

   Si utiliza la directiva de rutas de acceso **Fija**, podrá ver cuál es la ruta de acceso preferida. La ruta de acceso preferida se marca con un asterisco (*) en la columna Preferida.

Ver las rutas de acceso de los almacenes de datos

Revise las rutas de acceso que se conectan a los dispositivos de almacenamiento que respaldan a los almacenes de datos de VMFS.

Procedimiento

1 En vSphere Client, desplácese al almacén de datos.

2 Haga clic en la pestaña **Configurar**.

3 Haga clic en **Conectividad y habilitación de múltiples rutas**.

4 Seleccione un host para ver los detalles de múltiples rutas de sus dispositivos.

5 En Directivas de múltiples rutas, revise el módulo que posee el dispositivo, por ejemplo, NMP. También puede ver la directiva de selección de ruta de acceso y la directiva de tipo de matriz de almacenamiento asignada al dispositivo.

   Por ejemplo, es posible que vea lo siguiente:

Directiva de selección de ruta de acceso	Ruta de acceso preferida
Directiva de tipo de matriz de almacenamiento	VMW_SATP_LOCAL
Complemento de propietario	NMP

6 En Rutas de acceso, revise las rutas del dispositivo y el estado de cada ruta. Puede aparecer la siguiente información sobre el estado de la ruta de acceso:

Estado	Descripción
Activo (E/S)	Ruta de trabajo o múltiples rutas de acceso que actualmente transfieren datos.
En espera	Rutas de acceso inactivas. Si se produce un error en la ruta activa, pueden entrar en funcionamiento y comenzar a transferir E/S.
Deshabilitado	Rutas de acceso deshabilitadas por el administrador.
Inactiva	Rutas de acceso que ya no están disponibles para el procesamiento de E/S. Un error en un medio físico o la configuración incorrecta de una matriz pueden provocar este estado.

   Si utiliza la directiva de rutas de acceso **Fija**, podrá ver cuál es la ruta de acceso preferida. La ruta de acceso preferida se marca con un asterisco (*) en la columna Preferida.

Cambiar la directiva de selección de rutas de acceso

Generalmente, no es necesario cambiar la configuración predeterminada de múltiples rutas que usa el host ESXi para un dispositivo de almacenamiento específico. Si desea realizar cambios, puede utilizar el cuadro de diálogo **Editar directivas de múltiples rutas** para modificar una directiva de selección de ruta de acceso. También se puede utilizar este cuadro de diálogo para cambiar las múltiples rutas de los extremos de protocolo basado en SCSI.

Procedimiento

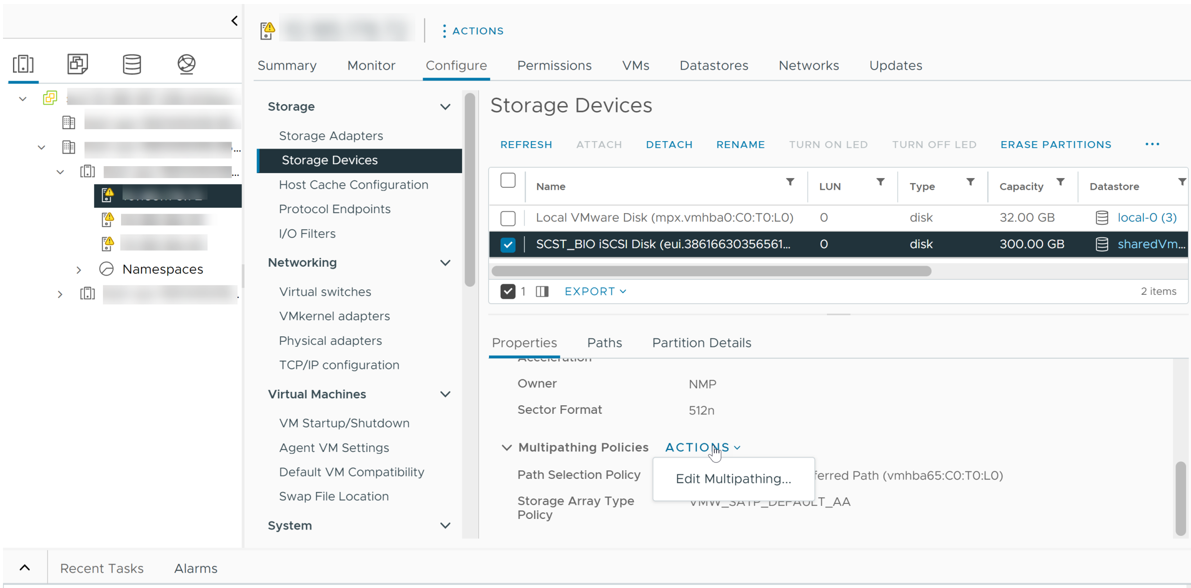
1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Dispositivos de almacenamiento** o **Extremos de protocolo**.

4 Seleccione el elemento cuyas rutas de acceso desea cambiar y haga clic en la pestaña **Propiedades**.

5 En Directivas de múltiples rutas, seleccione **Editar múltiples rutas** en el menú **Acciones**.



6 Seleccione una directiva de ruta de acceso y configure sus opciones. Las opciones cambian según el tipo de dispositivo de almacenamiento que se utilice.

- Para obtener información sobre las directivas de ruta de acceso para dispositivos SCSI, consulte Directivas y complementos de selección de rutas de acceso.
- Para obtener información sobre los mecanismos de ruta de acceso para dispositivos NVMe, consulte Complemento de alto rendimiento de VMware y esquemas de selección de rutas de acceso.

7 Para guardar la configuración y salir del cuadro de diálogo, haga clic en **Aceptar**.

Cambiar los parámetros predeterminados de una latencia de Round Robin

En el host ESXi, el mecanismo de latencia está activado de forma predeterminada para la directiva de selección de ruta de acceso de Round Robin. El mecanismo toma en cuenta la latencia de ruta de acceso y ancho de banda de E/S para seleccionar una ruta óptima para E/S. Cuando se utiliza el mecanismo de latencia, la directiva de Round Robin dinámicamente puede seleccionar la ruta óptima y lograr mejores resultados de equilibrio de carga.

Utilice el comando `esxcli` para cambiar los parámetros predeterminados del mecanismo de latencia o deshabilitar el mecanismo.

Requisitos previos

Establezca la directiva de selección de ruta de acceso en Round Robin. Consulte Cambiar la directiva de selección de rutas de acceso.

Procedimiento

1 Configure el mecanismo de latencia mediante el siguiente comando.

```
esxcli storage nmp psp roundrobin deviceconfig set --type=latency --device=device ID
```

El comando utiliza los siguientes parámetros:

Parámetro	Descripción
-S|--num-sampling-cycles=*sampling value*	Cuando `--type` se establece en `latency`, este parámetro controla cuántas operaciones de E/S se utilizan para calcular la latencia promedio de cada ruta de acceso. El valor predeterminado de este parámetro es 16.
-T|--latency-eval-time=*time in ms*	Cuando `--type` se establece en `latency`, este parámetro controla la frecuencia con que se actualiza la latencia de las rutas de acceso. El valor predeterminado es 3 minutos.

2 Compruebe si la latencia de Round Robin y sus parámetros están configurados correctamente.

```
esxcli storage nmp psp roundrobin deviceconfig get --device=device ID
```

o

```
esxcli storage nmp device list --device=device ID
```

Los resultados de ejemplo siguientes muestran la configuración de la ruta de acceso:

```
 Path Selection Policy: VMW_PSP_RR
   Path Selection Policy Device Config:
{policy=latency,latencyEvalTime=180000,samplingCycles=16,curSamplingCycle=16,useANO=0;
CurrentPath=vmhba1:C0:T0:L0: NumIOsPending=0,latency=0}
```

Pasos siguientes

Si quiere deshabilitar el mecanismo de latencia, en la configuración avanzada del sistema para el host, cambie el parámetro `Misc.EnablePSPLatencyPolicy` a 0.

Deshabilitar rutas de acceso de almacenamiento

Las rutas de acceso se pueden deshabilitar temporalmente para realizar mantenimiento o por otras razones.

Puede deshabilitar una ruta de acceso desde el panel Rutas de acceso. Existen varias formas de acceder al panel Rutas de acceso: desde un almacén de datos, un dispositivo de almacenamiento, un adaptador o una vista de punto de acceso de protocolo de Virtual Volumes.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en uno de los siguientes elementos:

- **Adaptadores de almacenamiento**
- **Dispositivos de almacenamiento**
- **Endpoints de protocolo**

4 En el panel derecho, seleccione el elemento cuyas rutas de acceso desee deshabilitar, un adaptador, un dispositivo de almacenamiento o un endpoint de protocolo y haga clic en la pestaña **Rutas de acceso**.

5 Seleccione la ruta de acceso que desea deshabilitar y haga clic en **Deshabilitar**.

El estado de la ruta de acceso cambia a Deshabilitado.

Usar reglas de notificación

Las reglas de notificación determinan qué módulo de múltiples rutas posee las rutas de acceso en un determinado dispositivo de almacenamiento. También definen el tipo de soporte de múltiples rutas que el host proporciona al dispositivo.

Las reglas de notificación se enumeran en el archivo `/etc/vmware/esx.conf` del host.

Las reglas se dividen en estas categorías:

Reglas de notificación de núcleo

Estas reglas de notificación determinan qué módulo de múltiples rutas (NMP, HPP o MPP de terceros) reclama el dispositivo específico.

Reglas de notificación de SATP

Según el tipo de dispositivo, estas reglas asignan un determinado submódulo SATP que proporciona administración de múltiples rutas específicas del proveedor al dispositivo.

Puede utilizar los comandos `esxcli` para agregar o cambiar el núcleo y las reglas de notificación de SATP. Por lo general, se agregan las reglas de notificación para cargar un MPP de terceros o para ocultar un LUN del host. Podría ser necesario cambiar las reglas de notificación cuando la configuración predeterminada de un dispositivo específico es insuficiente.

Para obtener más información sobre los comandos disponibles para administrar reglas de notificación de PSA, consulte *Introducción a ESXCLI*.

Para acceder a una lista de matrices de almacenamiento y sus correspondientes SATP y PSP, consulte la sección de almacenamiento/SAN de *vSphere Compatibility Guide*.

Consideraciones sobre múltiples rutas

Se aplican consideraciones específicas cuando se administran reglas de notificación y complementos de múltiples rutas de almacenamiento.

Las siguientes consideraciones serán útiles para la habilitación de múltiples rutas:

- Si no hay una SATP asignada al dispositivo por las reglas de notificación, la SATP predeterminada para dispositivos iSCSI o de canal de fibra es VMW_SATP_DEFAULT_AA. La PSP predeterminada es VMW_PSP_FIXED.
- Cuando el sistema busca las reglas de SATP con el fin de localizar una SATP para un determinado dispositivo, en primer lugar busca las reglas del controlador. Si no hay coincidencias, se buscan las reglas del proveedor/modelo y, por último, las reglas de transporte. Si no hay coincidencias, NMP selecciona la SATP predeterminada para el dispositivo.
- Si se asigna VMW_SATP_ALUA a un dispositivo de almacenamiento específico, pero el dispositivo no se basa en ALUA, no se producirán coincidencias de reglas de notificación para ese dispositivo. La SATP predeterminada reclama el dispositivo en función de su tipo de transporte.
- La PSP predeterminada para todos los dispositivos reclamados por VMW_SATP_ALUA es VMW_PSP_MRU. VMW_PSP_MRU selecciona una ruta de acceso activa/optimizada, según lo informado por VMW_SATP_ALUA, o bien una ruta de acceso activa/no optimizada en caso de que no haya una ruta activa/optimizada. Esta ruta de acceso se utiliza hasta que haya una ruta de acceso mejor disponible (MRU). Por ejemplo, si VMW_PSP_MRU actualmente utiliza una ruta de acceso activa/no optimizada y en algún momento hay una ruta de acceso activa/optimizada disponible, VMW_PSP_MRU pasará a utilizar esta última.
- Aunque por lo general se selecciona VMW_PSP_MRU para matrices ALUA de forma predeterminada, ciertas matrices de almacenamiento ALUA deben utilizar VMW_PSP_FIXED. Para comprobar si la matriz de almacenamiento requiere VMW_PSP_FIXED, consulte la *Guía de compatibilidad de VMware* o póngase en contacto con el proveedor de almacenamiento. Al utilizar VMW_PSP_FIXED con matrices ALUA, a menos que se especifique explícitamente una ruta de acceso preferida, el host ESXi selecciona la ruta de trabajo más óptima y la designa como ruta de acceso preferida predeterminada. Si la ruta seleccionada por el host deja de estar disponible, se seleccionará una ruta de acceso alternativa disponible. Sin embargo, si designa explícitamente la ruta de acceso preferida, seguirá siéndolo más allá de cuál sea su estado.
- De forma predeterminada, la regla de notificación de PSA 101 enmascara pseudodispositivos de matrices Dell. No elimine esta regla, a menos que quiera desenmascarar estos dispositivos.

Lista de reglas de notificación de múltiples rutas para el host

Utilice el comando `esxcli` para ver la lista de las reglas de notificación de múltiples rutas disponibles.

Las reglas de notificación indican si un NMP, HPP o MPP de terceros administran una ruta física determinada. Cada regla de notificación identifica un conjunto de rutas de acceso según los siguientes parámetros:

- Cadenas de proveedor/modelo

- Transporte, como SATA, IDE o canal de fibra
- Ubicación del adaptador, destino o LUN
- Controlador del dispositivo, por ejemplo, Mega-RAID

Procedimiento

- Para enumerar las reglas de notificación de múltiples rutas, ejecute el comando **esxcli storage core claimrule list --claimrule-class=MP**.

  Si no utiliza la opción claimrule-class, la clase de regla MP queda implícita.

Ejemplo: Resultados de muestra del comando esxcli storage core claimrule list

```
Rule Class  Rule   Class    Type       Plugin     Matches
MP           10    runtime  vendor     HPP        vendor=NVMe model=*
MP           10    file     vendor     HPP        vendor=NVMe model=*
MP           50    runtime  transport  NMP        transport=usb
MP           51    runtime  transport  NMP        transport=sata
MP           52    runtime  transport  NMP        transport=ide
MP           53    runtime  transport  NMP        transport=block
MP           54    runtime  transport  NMP        transport=unknown
MP          101    runtime  vendor     MASK_PATH  vendor=DELL model=Universal Xport
MP          101    file     vendor     MASK_PATH  vendor=DELL model=Universal Xport
MP          200    runtime  vendor     MPP_1      vendor=NewVend model=*
MP          200    file     vendor     MPP_1      vendor=NewVend model=*
MP          201    runtime  location   MPP_2      adapter=vmhba41 channel=* target=* lun=*
MP          201    file     location   MPP_2      adapter=vmhba41 channel=* target=* lun=*
MP          202    runtime  driver     MPP_3      driver=megaraid
MP          202    file     driver     MPP_3      driver=megaraid
MP          65535  runtime  vendor     NMP        vendor=* model=*
```

Este ejemplo indica lo siguiente:

- El NMP reclama todas las rutas de acceso conectadas a dispositivos de almacenamiento que utilizan transporte USB, SATA, IDE y SCSI en bloque.
- Se agregaron reglas para HPP, MPP_1, MPP_2 y MPP_3, a fin de que los módulos puedan reclamar dispositivos específicos. Por ejemplo, HPP reclama todos los dispositivos con NVMe de proveedor. Sin importar el proveedor real, se reclaman todos los dispositivos manejados por el controlador nvme de bandeja de entrada. El módulo MPP_1 reclama todas las rutas de acceso conectadas con cualquier modelo de la matriz de almacenamiento NewVend.
- Puede utilizar el módulo MASK_PATH para ocultar dispositivos no utilizados del host. De forma predeterminada, la regla de notificación de PSA 101 enmascara pseudodispositivos de matriz Dell con una cadena de proveedor DELL y una cadena de modelo Universal Xport.
- La columna Clase de regla en los resultados describe la categoría de la regla de notificación. Puede ser complemento de múltiples rutas (MP), filtro o VAAI.

- La columna Clase muestra qué reglas se definen y cuáles se cargan. El parámetro `file` en la columna Clase indica que la regla está definida. El parámetro `runtime` indica que la regla se cargó en el sistema. Para que una regla de notificación definida por el usuario se active, deben existir dos líneas con el mismo número de regla: una línea para la regla con el parámetro `file` y otra línea con `runtime`. Varias reglas de notificación predeterminadas definidas por el sistema tienen una sola línea con la clase de `runtime`. No se pueden modificar estas reglas.
- La regla predeterminada 65535 asigna todas las rutas de acceso sin reclamar a NMP. No elimine esta regla.

Agregar reglas de notificación de múltiples rutas

Utilice los comandos `esxcli` para agregar una regla de notificación de PSA de múltiples rutas al conjunto de reglas de notificación en el sistema. Para que la nueva regla de notificación sea activa, primero debe definir la regla y, a continuación, cargarla en el sistema.

A continuación se incluyen ejemplos de situaciones en las que se añade una regla de notificación de PSA:

- Carga un MPP de terceros nuevo y debe definir las rutas de acceso que reclama este módulo.
- Debe habilitar el complemento HPP nativo.

Advertencia No puede crear reglas donde dos complementos diferentes reclamen rutas de acceso al mismo dispositivo. Al intentar crear este tipo de reglas de notificación, se produce un error con una advertencia en `vmkernel.log`.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 Para definir una nueva regla de notificación, utilice el comando siguiente:

   `esxcli storage core claimrule add`

   El comando admite las siguientes opciones:

Opción	Descripción
-A|--adapter=<adapter>	Adaptador de las rutas de acceso que se utilizará. Válido únicamente si `--type` es `location`.
-u|--autoassign	Agrega una regla de notificación en función de sus características. El número de regla no es necesario.
-C|--channel=<channel>	Canal de las rutas de acceso que se utilizará. Válido únicamente si `--type` es `location`.

Opción	Descripción
-c|--claimrule-class=<cl>	Clase de regla de notificación que se utilizará en esta operación. Puede especificar `MP` (valor predeterminado), `Filter` o `VAAI`. A fin de configurar la aceleración de hardware para una nueva matriz, agregue dos reglas de notificación, una para el filtro VAAI y otra para el complemento VAAI. Consulte Agregar reglas de notificación de aceleración de hardware para obtener instrucciones detalladas.
-d|--device=<device_uid>	UID del dispositivo. Válido únicamente cuando `--type` es `device`.
-D|--driver=<driver>	Controlador para el HBA de las rutas de acceso que se utilizará. Válido únicamente si `--type` es `driver`.
-f|--force	Fuerce a las reglas de notificación a ignorar las comprobaciones de validez e instalar la regla de todas formas.
--force-reserved	Anule la protección de los rangos de identificadores de reglas reservadas. Las reglas de notificación reservadas son las reglas con un identificador inferior a 100. Puede utilizarlas para volver a asignar dispositivos locales a complementos específicos, por ejemplo, el dispositivo NVMe a HPP.
--if-unset=<str>	Ejecute este comando si esta variable de usuario avanzado no está establecida en 1.
-i|--iqn=<iscsi_name>	Nombre calificado de iSCSI para el destino. Válido únicamente cuando `--type` es `target`.
-L|--lun=<lun_id>	LUN de las rutas de acceso. Válido únicamente si `--type` es `location`. El identificador de LUN no debe ser mayor que el valor de la opción de configuración avanzada /Disk/MaxLUN.
-M|--model=<model>	Modelo de las rutas de acceso que se utilizará. Válido únicamente si `--type` es `vendor`. Los valores válidos son los valores de la cadena de modelo en la cadena de consulta de SCSI. Ejecute `vicfg-scsidevs <conn_options> -l` en cada dispositivo para ver los valores de cadena de modelo.
-P|--plugin=<plugin>	Complemento PSA que se utilizará. Los valores son `NMP`, `MASK_PATH` o `HPP`. Los terceros también pueden proporcionar sus propios complementos PSA. Requerido.
-r|--rule=<rule_ID>	Identificador de regla que se utilizará. El identificador de regla indica el orden en el que se evaluará la regla de notificación. Las reglas de notificación definidas por el usuario se evalúan en orden numérico a partir de 101. Puede ejecutar `esxcli storage core claimrule list` para determinar los identificadores de regla que deben estar disponibles.
-T|--target=<target>	Destino de las rutas de acceso que se utilizará. Válido únicamente si `--type` es `location`.

Opción	Descripción
-R|--transport=<transport>	Transporte de las rutas de acceso que se utilizará. Válido únicamente si `--type` es `transport`. Se admiten los siguientes valores. ■ `block`: almacenamiento en bloque ■ `fc`: canal de fibra ■ `iscsivendor`: iSCSI ■ `iscsi`: no se encuentra en uso ■ `ide`: almacenamiento IDE ■ `sas`: almacenamiento SAS ■ `sata`: almacenamiento SATA ■ `usb`: almacenamiento USB ■ `parallel`: paralelo ■ `fcoe`: FCoE ■ `unknown`
-t|--type=<type>	Tipo de coincidencia que se utilizará para la operación. Los valores válidos son los siguientes. Requerido. ■ `vendor` ■ `location` ■ `driver` ■ `transport` ■ `device` ■ `target`
-V|--vendor=<vendor>	Proveedor de las rutas de acceso que se utilizará. Válido únicamente si `--type` es `vendor`. Los valores válidos son los valores de la cadena de proveedor en la cadena de consulta de SCSI. Ejecute `vicfg-scsidevs <conn_options> -l` en cada dispositivo para ver los valores de cadena de proveedor.
--wwnn=<wwnn>	Número de nodo a escala mundial para el destino.
--wwpn=<wwpn>	Número de puerto a escala mundial para el destino.
-a|--xcopy-use-array-values	Utilice los valores informados por la matriz para construir el comando XCOPY que se enviará a la matriz de almacenamiento. Esto se aplica únicamente a las reglas de notificación VAAI.
-s|--xcopy-use-multi-segs	Utilice varios segmentos al emitir una solicitud XCOPY. Válido únicamente si se especifica `--xcopy-use-array-values`.
-m|--xcopy-max-transfer-size	Tamaño máximo de transferencia de datos en MB cuando se utiliza un tamaño de transferencia diferente al informado por la matriz. Válido únicamente si se especifica `--xcopy-use-array-values`.
-k|--xcopy-max-transfer-size-kib	Tamaño máximo de transferencia en KiB para los comandos XCOPY cuando se utiliza un tamaño de transferencia diferente al informado por la matriz. Válido únicamente si se especifica `--xcopy-use-array-values`.

2 Para cargar la nueva regla de notificación en el sistema, utilice el siguiente comando:

```
esxcli storage core claimrule load
```

Este comando carga todas las reglas de notificación de múltiples rutas recientemente creadas del archivo de configuración `esx.conf` al VMkernel. El comando no tiene opciones.

3 Para aplicar las reglas de notificación cargadas, utilice el siguiente comando:

`esxcli storage core claimrule run`

El comando admite las siguientes opciones:

Opción	Descripción
-A|--adapter=<adapter>	Si `--type` es `location`, el nombre del HBA para las rutas de acceso en las que se ejecutarán las reglas de notificación. Para ejecutar las reglas de notificación en rutas de acceso de todos los adaptadores, omita esta opción.
-C|--channel=<channel>	Si `--type` es `location`, el valor del número de canal SCSI para las rutas de acceso en las que se ejecutarán las reglas de notificación. Para ejecutar las reglas de notificación en rutas de acceso con cualquier número de canal, omita esta opción.
-c|--claimrule-class=<cl>	Clase de regla de notificación que se utilizará en esta operación.
-d|--device=<device_uid>	UID del dispositivo.
-L|--lun=<lun_id>	Si `--type` es `location`, el valor del LUN de SCSI para las rutas de acceso en las que se ejecutarán las reglas de notificación. Para ejecutar las reglas de notificación en rutas de acceso con cualquier LUN, omita esta opción.
-p|--path=<path_uid>	Si `--type` es `path`, esta opción indica el identificador único de ruta de acceso (Unique Path Identifier, UID) o el nombre de tiempo de ejecución de una ruta de acceso en la que se ejecutarán las reglas de notificación.
-T|--target=<target>	Si `--type` es `location`, el valor del número de destino SCSI para las rutas de acceso en las que se ejecutarán las reglas de notificación. Para ejecutar las reglas de notificación en rutas de acceso con cualquier número de destino, omita esta opción.
-t|--type=<location|path|all>	Tipo de notificación que se ejecutará. De forma predeterminada, se utiliza `all`, lo que significa que las reglas de notificación se ejecutan sin restricción de rutas de acceso específicas o direcciones de SCSI. Los valores válidos son `location`, `path` y `all`.
-w|--wait	Puede utilizar esta opción únicamente si también utiliza `--type all`. Si se incluye la opción, la notificación espera que las rutas de acceso se asienten antes de ejecutar la operación de notificación. En ese caso, el sistema no iniciará el proceso de notificación hasta que sea factible que todas las rutas de acceso hayan aparecido en el sistema antes de iniciar el proceso de notificación. Después de que se inicia el proceso de notificación, el comando no devuelve resultados hasta que se completa el registro del dispositivo. Si se agregan o eliminan rutas de acceso durante el proceso de notificación o detección, es posible que esta opción no funcione correctamente.

Ejemplo: Definir reglas de notificación de múltiples rutas

En el siguiente ejemplo, se agrega y se carga la regla n.º 500. La regla notifica todas las rutas de acceso con la cadena del modelo NewMod y la cadena del proveedor NewVend para el complemento NMP.

esxcli storage core claimrule add -r 500 -t vendor -V NewVend -M NewMod -P NMP

esxcli storage core claimrule load

Después de ejecutar el comando **esxcli storage core claimrule list**, verá la nueva regla de notificación en la lista.

El siguiente resultado indica que la regla de notificación 500 se ha cargado en el sistema y está activa.

```
Rule Class  Rule   Class    Type       Plugin     Matches
...         ...    ...      ...        ...        ...
MP          500    runtime  vendor     NMP        vendor=NewVend model=NewMod
MP          500    file     vendor     NMP        vendor=NewVend model=NewMod
```

Eliminar reglas de notificación de múltiples rutas

Utilice los comandos `esxcli` para quitar una regla de notificación de PSA de múltiples rutas del conjunto de reglas de notificación en el sistema.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 Elimine una regla de notificación del conjunto de reglas de notificación.

esxcli storage core claimrule remove

Nota De forma predeterminada, la regla de notificación de PSA 101 enmascara pseudodispositivos de matrices Dell. No elimine esta regla, a menos que quiera desenmascarar estos dispositivos.

El comando admite las siguientes opciones:

Opción	Descripción
-c|--claimrule-class=<str>	Indique la clase de regla de notificación (MP, filtro, VAAI).
-P|--plugin=<str>	Indique el complemento.
-r|--rule=<long>	Indique el identificador de la regla.

Este paso quita la regla de notificación de la clase Archivo.

2 Quite la regla de notificación del sistema.

   esxcli storage core claimrule load

   Este paso quita la regla de notificación de la clase Tiempo de ejecución.

Enmascarar rutas de acceso

Se puede evitar que el host acceda a los dispositivos de almacenamiento o LUN, o que utilice rutas de acceso individuales a un LUN. Utilice los comandos `esxcli` para enmascarar las rutas de acceso. Cuando se enmascaran rutas de acceso, se crean reglas de notificación que asignan el complemento MASK_PATH a las rutas de acceso especificadas.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 Compruebe cuál es el próximo identificador de regla disponible.

   esxcli storage core claimrule list

   Las reglas de notificación que se usan para enmascarar rutas tienen identificadores de regla dentro del rango de 101 a 200. Si este comando muestra que ya existen las reglas 101 y 102, puede especificar 103 para la regla que desee agregar.

2 Asigne el complemento MASK_PATH a una ruta de acceso. Para ello, cree una regla de notificación nueva para el complemento.

   esxcli storage core claimrule add -P MASK_PATH

3 Cargue la regla de notificación MASK_PATH en el sistema.

   esxcli storage core claimrule load

4 Compruebe que la regla de notificación MASK_PATH se haya agregado correctamente.

   esxcli storage core claimrule list

5 Si hay una regla de notificación para la ruta de acceso enmascarada, quítela.

   esxcli storage core claiming unclaim

6 Ejecute las reglas de notificación de ruta de acceso.

   esxcli storage core claimrule run

Resultados

Una vez asignado el complemento MASK_PATH a una ruta de acceso, el estado de la ruta de acceso se vuelve irrelevante y el host deja de mantenerlo. Como resultado, los comandos que muestran la información de la ruta de acceso enmascarada pueden mostrar el estado de la ruta de acceso como inactivo.

Ejemplo: Enmascaramiento de un LUN

En este ejemplo, se enmascara el LUN 20 en los destinos T1 y T2, a los que se accede a través de los adaptadores de almacenamiento vmhba2 y vmhba3.

1
```
#esxcli storage core claimrule list
```

2
```
#esxcli storage core claimrule add -P MASK_PATH -r 109 -t location -A vmhba2 -C 0 -T 1 -L 20
#esxcli storage core claimrule add -P MASK_PATH -r 110 -t location -A vmhba3 -C 0 -T 1 -L 20
#esxcli storage core claimrule add -P MASK_PATH -r 111 -t location -A vmhba2 -C 0 -T 2 -L 20
#esxcli storage core claimrule add -P MASK_PATH -r 112 -t location -A vmhba3 -C 0 -T 2 -L 20
```

3
```
#esxcli storage core claimrule load
```

4
```
#esxcli storage core claimrule list
```

5
```
#esxcli storage core claiming unclaim -t location -A vmhba2
#esxcli storage core claiming unclaim -t location -A vmhba3
```

6
```
#esxcli storage core claimrule run
```

Desenmascarar rutas de acceso

Cuando necesite que el host tenga acceso al dispositivo de almacenamiento enmascarado, quite la máscara de las rutas al dispositivo.

Nota Cuando se ejecuta una operación de anulación de notificación con una propiedad del dispositivo, por ejemplo, el identificador de dispositivo o el proveedor, no se anula la notificación de las rutas de acceso que reclama el complemento MASK_PATH. El complemento MASK_PATH no realiza un seguimiento de ninguna propiedad del dispositivo de las rutas de acceso que notifica.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 Elimine la regla de notificación MASK_PATH.

   `esxcli storage core claimrule remove -r rule#`

2 Compruebe que la regla de notificación se haya eliminado correctamente.

   `esxcli storage core claimrule list`

3 Vuelva a cargar las reglas de notificación de ruta de acceso del archivo de configuración al VMkernel.

esxcli storage core claimrule load

4 Ejecute el comando **esxcli storage core claiming unclaim** para cada ruta de acceso al dispositivo de almacenamiento enmascarado.

Por ejemplo:

esxcli storage core claiming unclaim -t location -A vmhba0 -C 0 -T 0 -L 149

5 Ejecute las reglas de notificación de ruta de acceso.

esxcli storage core claimrule run

Resultados

El host ahora puede acceder al dispositivo de almacenamiento que estaba enmascarado.

Definir reglas de SATP de NMP

Las reglas de notificación de SATP de NMP definen cuál SATP administra un dispositivo de almacenamiento. Por lo general, puede utilizar los SATP predeterminados que se proporcionan para los dispositivos de almacenamiento. Si la configuración predeterminada no es suficiente, utilice los comandos `esxcli` para cambiar el SATP de un dispositivo específico.

Es posible que necesite crear una regla de SATP al instalar un SATP de terceros para una matriz de almacenamiento específica.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 A fin de agregar una regla de notificación para un SATP específico, ejecute el comando **esxcli storage nmp satp rule add**. El comando acepta las opciones siguientes.

Opción	Descripción
-b|--boot	Se trata de una regla predeterminada del sistema que se agrega en el momento del arranque. No modifique `esx.conf` ni agregue nada a un perfil de host.
-c|--claim-option=*string*	Establezca la cadena de opción de notificación cuando agrega una regla de notificación de SATP.
-e|--description=*string*	Establezca la descripción de la regla de notificación cuando agrega una regla de notificación de SATP.
-d|--device=*string*	Establezca el dispositivo cuando agrega reglas de notificación de SATP. Las reglas del dispositivo son mutuamente exclusivas con las reglas del proveedor/modelo y del controlador.

Opción	Descripción
-D|--driver=*string*	Establezca la cadena del controlador cuando agrega una regla de notificación de SATP. Las reglas del controlador son mutuamente exclusivas con las reglas del proveedor/modelo.
-f|--force	Fuerce a las reglas de notificación a ignorar las comprobaciones de validez e instalar la regla de todas formas.
-h|--help	Muestre el mensaje de ayuda.
-M|--model=*string*	Establezca la cadena del modelo cuando agrega una regla de notificación a SATP. Las reglas del proveedor/modelo son mutuamente exclusivas con las reglas del controlador.
-o|--option=*string*	Establezca la cadena de opción cuando agrega una regla de notificación de SATP.
-P|--psp=*string*	Establezca el PSP predeterminado para la regla de notificación de SATP.
-O|--psp-option=*string*	Establezca las opciones del PSP para la regla de notificación de SATP.
-s|--satp=*string*	El SATP para el que se ha agregado una regla nueva.
-R|--transport=*string*	Establezca la cadena de tipo de transporte de notificación cuando agrega una regla de notificación de SATP.
-t|--type=*string*	Establezca el tipo de cadena cuando agrega una regla de notificación de SATP.
-V|--vendor=*string*	Establezca la cadena del proveedor cuando agrega reglas de notificación de SATP. Las reglas del proveedor/modelo son mutuamente exclusivas con las reglas del controlador.

Nota Cuando busca las reglas de SATP para ubicar un SATP de un dispositivo dado, el NMP busca primero las reglas del controlador. Si no hay coincidencia, se buscan las reglas del proveedor/modelo y, por último, las reglas de transporte. Si aún no hay coincidencia, el NMP selecciona un SATP predeterminado para el dispositivo.

2 Reinicie el host.

Ejemplo: Definir una regla de SATP de NMP

El comando de muestra siguiente asigna el complemento VMW_SATP_INV para administrar las matrices de almacenamiento con la cadena del proveedor NewVend y la cadena del modelo NewMod.

```
# esxcli storage nmp satp rule add -V NewVend -M NewMod -s VMW_SATP_INV
```

Cuando ejecute el comando **esxcli storage nmp satp list -s VMW_SATP_INV**, podrá ver que la regla nueva se agregó a la lista de reglas VMW_SATP_INV.

Colas de programación de E/S de máquinas virtuales

De forma predeterminada, vSphere proporciona un mecanismo que crea colas de programación para cada archivo de máquina virtual. Cada archivo, por ejemplo, `.vmdk`, obtiene sus propios controles de ancho de banda.

Este mecanismo asegura que la E/S de un archivo de máquina virtual específico vaya a su propia cola separada, y evita que interfiera con las operaciones de E/S de otros archivos.

Esta funcionalidad está habilitada de forma predeterminada. Puede usar los comandos de vSphere Client o `esxcli` para deshabilitar o volver a habilitar la capacidad.

Editar programación de E/S por archivo en vSphere Client

El parámetro de `VMkernel.Boot.isPerFileSchedModelActive` avanzado controla el mecanismo de programación de E/S por archivo en los almacenes de datos de VMFS y NFS 3. En el host ESXi, el mecanismo está habilitado de forma predeterminada. Puede deshabilitar el mecanismo mediante el cuadro de diálogo **Configuración avanzada del sistema**.

Si se desactiva el modelo de programación de E/S por archivo, el host se revierte a un mecanismo de programación heredado. La programación heredada mantiene una única cola de E/S para cada par de máquina virtual y dispositivo de almacenamiento. Todas las E/S entre la máquina virtual y sus discos virtuales se trasladan a esta cola. Como resultado, las E/S de distintos discos virtuales pueden interferir entre sí al compartir el ancho de banda y afectar el rendimiento de las otras.

Nota No deshabilite la programación por archivo si el complemento HPP y el parámetro de umbral sensible de latencia están configurados para dispositivos locales de alta velocidad. Si la deshabilita, puede provocar un comportamiento impredecible.

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Sistema**, haga clic en **Configuración avanzada del sistema**.
4. Edite el valor del parámetro **VMkernel.Boot.isPerFileSchedModelActive**.

Opción	Descripción
False	Deshabilite el mecanismo de programación por archivo.
True (valor predeterminado)	Vuelva a habilitar el mecanismo de programación por archivo.

5. Reinicie el host para que se apliquen los cambios.

Utilizar comandos esxcli para habilitar o deshabilitar la programación de E/S por archivo

Puede usar los comandos de `esxcli` para cambiar la capacidad de programación de E/S para almacenes de datos de VMFS, NFS 3 y NFS 4.1 en el host ESXi. La funcionalidad está habilitada de forma predeterminada.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

- Para habilitar o deshabilitar la programación de E/S por archivo, ejecute los siguientes comandos:

Opción	Descripción
esxcli system settings kernel set -s isPerFileSchedModelActive -v FALSE	Deshabilite la programación de E/S por archivo para VMFS y NFS 3.
esxcli system settings kernel set -s isPerFileSchedModelActive -v TRUE	Habilite la programación de E/S por archivo para VMFS y NFS 3.
esxcli system module parameters list -m nfs41client	Enumera el estado actual del programador basado en archivos NFS 4.1
esxcli system module parameters set -m nfs41client -p fileBasedScheduler=0	Deshabilite el programador basado en archivos para NFS 4.1.
esxcli system module parameters set -m nfs41client -p fileBasedScheduler=1	Habilite el programador basado en archivos para NFS 4.1.

Asignación de dispositivos sin formato

19

La asignación de dispositivos sin formato (RDM) proporciona un mecanismo para que la máquina virtual tenga acceso directo al LUN en el subsistema de almacenamiento físico.

Los siguientes temas contienen información sobre RDM y ofrecen instrucciones sobre cómo crear y administrar RDM.

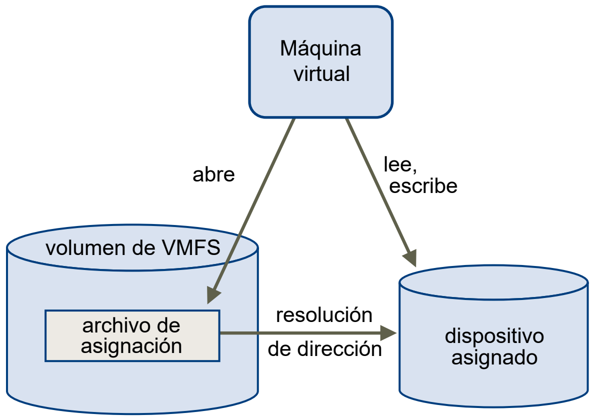
Este capítulo incluye los siguientes temas:

Acerca de la asignación de dispositivos sin formato

El RDM es un archivo de asignación en un volumen VMFS distinto que actúa como proxy de un dispositivo de almacenamiento físico sin formato. Con el RDM, una máquina virtual puede acceder y utilizar el dispositivo de almacenamiento directamente. El RDM contiene metadatos para administrar y redirigir el acceso del disco al dispositivo físico.

El archivo proporciona algunas de las ventajas del acceso directo a un dispositivo físico, pero mantiene algunas ventajas de un disco virtual en VMFS. Como resultado, combina la capacidad de administración de VMFS con el acceso de dispositivos sin formato.

Figura 19-1. Asignar dispositivos sin formato



Por lo general, los almacenes de datos VMFS se usan en la mayoría de casos de almacenamiento en disco virtual. En ciertas ocasiones, se pueden utilizar LUN sin formato o discos lógicos ubicados en un SAN.

Por ejemplo, se pueden utilizar LUN sin formato con RDM en las situaciones siguientes:

- Cuando una snapshot de SAN u otras aplicaciones en capas se ejecutan en la máquina virtual. El RDM habilita los sistemas de descarga de copia de seguridad con la utilización de características inherentes a la SAN.
- En cualquier escenario de agrupación en clústeres de MSCS que comprenda hosts físicos, como clústeres virtual a virtual y clústeres físico a virtual. En este caso, los datos de clúster y los discos de quórum se configuran como RDM en lugar de como discos virtuales en un VMFS compartido.

Piense en un RDM como un vínculo simbólico de un volumen VMFS a un LUN sin formato. La asignación hace que los LUN aparezcan como archivos en un volumen VMFS. Al RDM, no al LUN sin formato, se hace referencia en la configuración de la máquina virtual. El RDM contiene una referencia al LUN sin formato.

Hay dos modos de compatibilidad disponibles para los RDM:

- En el modo de compatibilidad virtual, el RDM actúa como un archivo de disco virtual. El RDM puede usar instantáneas.
- En el modo de compatibilidad física, el RDM ofrece acceso directo al dispositivo SCSI para aquellas aplicaciones que requieren un control de nivel inferior.

Beneficios de la asignación de dispositivos sin formato

Un RDM proporciona varios beneficios, pero no debe utilizarse en todas las situaciones. En general, los archivos de disco virtual son preferibles a los RDM gracias a su manejabilidad. Sin embargo, cuando se necesitan dispositivos sin procesar, debe usar el RDM.

El RDM ofrece varios beneficios.

Nombres persistentes descriptivos

Proporciona un nombre fácil para un dispositivo asignado. Cuando utiliza el RDM, no es necesario referirse al dispositivo por su nombre de dispositivo. Se puede referir a este por el nombre del archivo de asignación, por ejemplo:

```
/vmfs/volumes/myVolume/myVMDirectory/myRawDisk.vmdk
```

Resolución de nombres dinámica

Almacena información de identificación única de cada dispositivo asignado. VMFS asocia cada RDM con su dispositivo SCSI actual, independientemente de los cambios en la configuración física del servidor debido a cambios en el hardware del adaptador, cambios de rutas de acceso, reubicación del dispositivo, etc.

Bloqueo de archivos distribuido

Permite usar el bloqueo distribuido de VMFS para dispositivos SCSI sin procesar. El bloqueo distribuido en un RDM hace que sea seguro usar un LUN sin procesar compartido sin perder datos cuando dos máquinas virtuales en distintos servidores intentan acceder al mismo LUN.

Permisos de archivo

Posibilita los permisos de archivo. Los permisos del archivo de asignación se implementan en el momento de abrir el archivo para proteger el volumen asignado.

Operaciones del sistema de archivos

Permite usar las utilidades del sistema de archivos para trabajar con un volumen asignado, usando el archivo de asignación como proxy. La mayoría de las operaciones que son válidas para un archivo común pueden aplicarse al archivo de asignación y se redireccionan para funcionar en el dispositivo asignado.

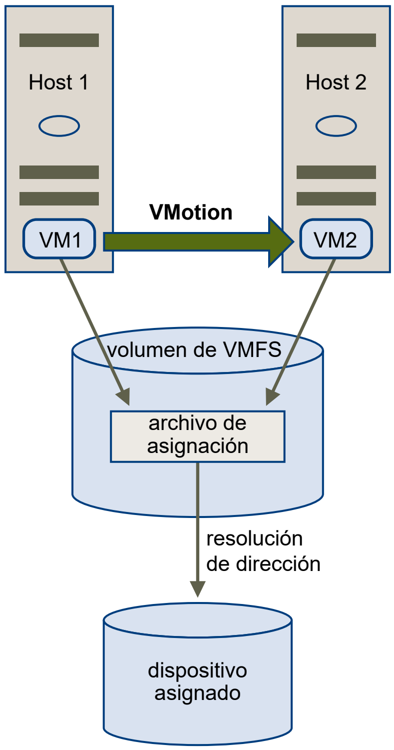
Snapshots

Posibilita usar snapshots de máquina virtual en un volumen asignado. Las snapshots no están disponibles cuando el RDM se usa en modo de compatibilidad física.

vMotion

Permite migrar una máquina virtual con vMotion. El archivo de asignación actúa como proxy para permitir a vCenter Server migrar la máquina virtual con el mismo mecanismo que para migrar archivos de disco virtual.

Figura 19-2. vMotion de una máquina virtual con asignación de dispositivos sin formato



Agentes de administración de SAN

Posibilita ejecutar algunos agentes de administración de SAN dentro de una máquina virtual. De manera similar, cualquier software que necesita acceder a un dispositivo mediante comandos SCSI específicos de hardware puede ejecutarse en una máquina virtual. Este tipo de software se denomina software basado en destino de SCSI. Cuando usa agentes de administración de SAN, seleccione un modo de compatibilidad física para el RDM.

Virtualización de identificador de puerto N (NPIV).

Posibilita usar la tecnología NPIV que permite que un puerto HBA de canal de fibra único se registre en el tejido de canal de fibra con varios nombres de puertos universales (WWPN). Esta capacidad hace que el puerto HBA aparezca como varios puertos virtuales, cada uno con su propio identificador y nombre de puerto virtual. Las máquinas virtuales pueden, a continuación, reclamar cada uno de estos puertos y usarlos para todo el tráfico RDM.

Nota Puede usar NPIV solo para máquinas virtuales con discos RDM.

VMware funciona con proveedores de software de administración de almacenamiento para asegurar que su software funcione correctamente en entornos que incluyen ESXi. Algunas aplicaciones de este tipo son:

- software de administración de SAN
- Software de administración de recursos de almacenamiento (SRM)
- Software de snapshots

- Software de replicación

Este tipo de software usa un modo de compatibilidad física para los RDM de modo que el software pueda acceder a dispositivos SCSI directamente.

Varios productos de administración se ejecutan mejor de forma centralizada (no en la máquina de ESXi), mientras que otros se ejecutan bien en las máquinas virtuales. VMware no certifica estas aplicaciones ni proporciona una matriz de compatibilidad. Para saber si una aplicación de administración de SAN es compatible con un entorno de ESXi, póngase en contacto con el proveedor de software de administración de SAN.

Consideraciones y limitaciones de RDM

Al usar los RDM, hay que tener en cuenta ciertas consideraciones y limitaciones.

- El RDM no está disponible para los dispositivos de bloque de conexión directa ni para ciertos dispositivos RAID. El RDM usa un número de serie de SCSI para identificar el dispositivo asignado. Debido a que los dispositivos de bloque y algunos dispositivos RAID de conexión directa no exportan números de serie, no se pueden utilizar con los RDM.
- Si utiliza el RDM en el modo de compatibilidad física, no puede utilizar una snapshot con el disco. El modo de compatibilidad física permite a la máquina virtual administrar sus propias operaciones de creación de snapshots o de reflejos basadas en almacenamiento.

  Las snapshots de máquina virtual están disponibles para RDM con modo de compatibilidad virtual.
- No se puede realizar una asignación a una partición de disco. Los RDM requieren que el dispositivo asignado sea un LUN completo.
- Si usa vMotion para migrar máquinas virtuales con RDM, asegúrese de que los identificadores de LUN sean coherentes para los RDM en todos los hosts ESXi implicados.

Características de la asignación de dispositivos sin formato

RDM es un archivo de asignación especial en un volumen VMFS que administra metadatos para su dispositivo asignado. El archivo de asignación se presenta ante el software de administración como un archivo común del disco, disponible para las operaciones normales del sistema de archivos. Para la máquina virtual, la capa de virtualización de almacenamiento presenta el dispositivo asignado como un dispositivo SCSI virtual.

Entre el contenido clave de los metadatos en el archivo de asignación se encuentran la ubicación del dispositivo asignado (resolución de nombres), el estado de bloqueo del dispositivo asignado, los permisos, etc.

Modos de compatibilidad virtual y física de RDM

Puede utilizar RDM en los modos de compatibilidad virtual o compatibilidad física. El modo virtual especifica la virtualización completa del dispositivo asignado. El modo físico especifica una

virtualización SCSI mínima del dispositivo asignado y permite la mayor flexibilidad del software de administración de SAN.

En el modo virtual, el VMkernel envía solo READ y WRITE al dispositivo asignado. Para el sistema operativo invitado, el dispositivo asignado aparece exactamente igual que un archivo de disco virtual en un volumen VMFS. Las características reales de hardware están ocultas. Si utiliza un disco sin formato en modo virtual, puede aprovechar los beneficios de VMFS, como el bloqueo avanzado de archivos para protección de datos y las snapshots para optimizar los procesos de desarrollo. El modo virtual también es más portátil en hardware de almacenamiento que en el modo físico, ya que presenta el mismo comportamiento que un archivo de disco virtual.

En el modo físico, el VMkernel transfiere todos los comandos SCSI al dispositivo, salvo uno: el comando REPORT LUN está virtualizado, de modo que el VMkernel puede aislar el LUN en la máquina virtual al que le pertenece. Caso contrario, se exponen todas las características físicas del hardware subyacente. El modo físico es útil para ejecutar agentes de administración de SAN u otro software basado en destinos SCSI en la máquina virtual. El modo físico también permite la agrupación en clústeres virtual a física para obtener una alta disponibilidad rentable.

VMFS5 y VMFS6 son compatibles con tamaños de disco superiores a 2 TB para RDM en los modos virtual y físico.

Resolución de nombres dinámica

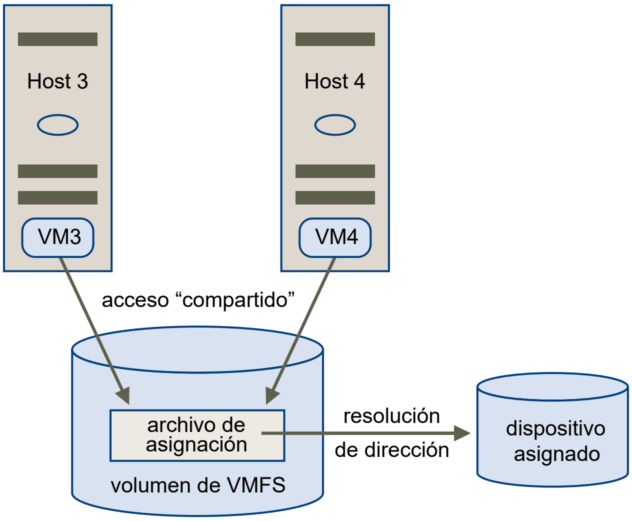
El archivo RDM admite la resolución de nombres dinámica cuando cambia la ruta de acceso a un dispositivo sin formato.

VMFS identifica de manera única todos los dispositivos de almacenamiento asignados y la identificación se almacena en sus estructuras de datos internas. Cualquier cambio en la ruta de acceso a un dispositivo sin formato, como un error en un conmutador de canal de fibra o el agregado de un HBA nuevo, puede cambiar el nombre del dispositivo. La resolución de nombres dinámica resuelve estos cambios y asocia automáticamente el dispositivo original con su nuevo nombre.

Asignación de dispositivos sin formato con clústeres de máquinas virtuales

Utilice el RDM con clústeres de máquinas virtuales que necesitan acceder al mismo LUN sin procesar en caso de ocurra conmutación por error. La configuración es similar a la de un clúster de máquina virtual que accede al mismo archivo de disco virtual, pero el RDM reemplaza el archivo del disco virtual.

Figura 19-3. Acceder desde máquinas virtuales con clúster



Comparar modos de acceso de dispositivos SCSI disponibles

Es posible acceder a un dispositivo de almacenamiento basado en SCSI mediante un archivo de disco virtual en un almacén de datos de VMFS, un RDM de modo virtual o un RDM de modo físico.

En la siguiente tabla se proporciona una comparación de las características disponibles con los diferentes modos.

Tabla 19-1. Características disponibles con asignaciones de discos virtuales y dispositivos sin formato

Características de ESXi	Archivo de disco virtual	RDM de modo virtual	RDM de modo físico
Comandos SCSI transmitidos	No	No	Sí Los `REPORT LUNs` no se han transmitido
Soporte de vCenter Server	Sí	Sí	Sí
Snapshots	Sí	Sí	No
Bloqueo distribuido	Sí	Sí	Sí
Agrupar en clústeres	Solo sistemas Cluster-in-a-box	Sistema Cluster-in-a-box sistema Cluster-across-boxes	Agrupación en clústeres física a virtual sistema Cluster-across-boxes
Software basado en destinos de SCSI	No	No	Sí

Utilice archivos de disco virtual para el tipo de clúster de sistema Cluster-in-a-box. Si planea reconfigurar los clústeres de sistema Cluster-in-a-box, como clústeres de sistema Cluster-across-boxes, use el RDM de modo virtual para los clústeres de sistema Cluster-in-a-box.

Crear máquinas virtuales con RDM

Al otorgarle a la máquina virtual acceso directo a un LUN de SAN sin procesar, crea un disco RDM que reside en un almacén de datos de VMFS y que apunta al LUN. El RDM se crea como un disco inicial para una máquina virtual nueva o se agrega a una máquina virtual existente. Al crear el RDM, se especifica el LUN que se va a asignar y el almacén de datos en el que se debe colocar la RDM.

Aunque el archivo de disco RDM tiene la misma extensión `.vmdk` que un archivo de disco virtual normal, el RDM contiene solo información de asignación. Los datos del disco virtual actual se almacenan directamente en el LUN.

Este procedimiento da por sentado que se está creando una máquina virtual nueva. Para obtener información, consulte el documento *Administrar máquinas virtuales de vSphere*.

Procedimiento

1 Cree una máquina virtual.

   a Haga clic con el botón derecho en cualquier objeto de inventario que sea un objeto principal válido de una máquina virtual, como un centro de datos, una carpeta, un clúster, un grupo de recursos o un host, y seleccione **Nueva máquina virtual**.

   b Seleccione **Crear una nueva máquina virtual** y haga clic en **Siguiente**.

   c Siga los pasos necesarios para crear una máquina virtual.

2 En la página Personalizar hardware, haga clic en la pestaña **Hardware virtual**.

3 (opcional) Para eliminar el disco duro virtual predeterminado que creó el sistema para la máquina virtual, mueva el cursor sobre el disco y haga clic en el icono **Quitar**.

4 Agregue un disco RDM.

   a Haga clic en **Agregar nuevos dispositivos** y seleccione **Disco RDM** en la lista.

   b En la lista de los LUN, seleccione el LUN sin procesar de destino y haga clic en **Aceptar**.

   El sistema crea un disco RDM que asigna la máquina virtual al LUN de destino. El disco RDM se muestra en la lista de dispositivos virtuales como un disco duro nuevo.

5 Configure el disco RDM.

   a Haga clic en el triángulo **Nuevo disco duro** para expandir las propiedades del disco RDM.

   b Seleccione una ubicación para el RDM.

   Puede colocar el RDM en el mismo almacén de datos en el que residen los archivos de configuración de la máquina virtual o seleccionar un almacén de datos distinto.

   Nota Para utilizar vMotion en máquinas virtuales con NPIV habilitada, asegúrese de que los archivos RDM y los archivos de máquina virtual se encuentren en el mismo almacén de datos. No es posible ejecutar Storage vMotion cuando la funcionalidad de NPIV está habilitada.

c Seleccione un modo de compatibilidad.

Opción	Descripción
Físico	Permite que el sistema operativo invitado acceda al hardware en forma directa. La compatibilidad física resulta útil cuando se usan aplicaciones basadas en SAN en la máquina virtual. No obstante, no es posible clonar una máquina virtual con RDM de compatibilidad física, crear una plantilla a partir de ella ni migrarla si la migración implica realizar una copia en el disco.
Virtual	Permite que el disco RDM se comporte como un disco virtual, para que se puedan utilizar características como creación de snapshots, clonación, etc. Cuando se clona el disco para crear una plantilla a partir de él, el contenido del LUN se copia en un archivo de disco virtual `.vmdk`. Cuando se migra un disco RDM en modo de compatibilidad virtual, es posible migrar el archivo de asignación a un disco virtual o copiar el contenido del LUN en un disco virtual.

d Si seleccionó el modo de compatibilidad virtual, seleccione un modo de disco.

Los modos de discos no están disponibles para los discos RDM que usan el modo de compatibilidad física.

Opción	Descripción
Dependiente	Se incluyen discos dependientes en las instantáneas.
Independiente persistente	Los discos en modo persistente se comportan como los discos convencionales en el equipo físico. Todos los datos que se escriben en un disco en modo persistente se escriben de forma permanente en el disco.
Independiente no persistente	Los cambios en los discos en modo no persistente se descartan cuando se apaga o se restablece la máquina virtual. Con el modo no persistente, puede reiniciar la máquina virtual con un disco virtual en el mismo estado cada vez. Los cambios en el disco se escriben y se leen desde un archivo de registro de rehacer que se elimina al apagar o restablecer.

6 Complete la configuración de la máquina virtual.

Administrar rutas de acceso para un LUN asignado

Cuando utiliza máquinas virtuales con RDM, puede administrar rutas de acceso para los LUN sin formato asignados.

Procedimiento

1 Haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.
2 Haga clic en la pestaña **Hardware virtual** y, a continuación, haga clic en **Disco duro** para expandir el menú de opciones del disco.
3 Haga clic en el identificador del dispositivo que aparece junto a **LUN físico** para abrir el cuadro de diálogo **Editar directivas de múltiples rutas**.

4 Utilice el cuadro de diálogo **Editar directivas de múltiples rutas** para habilitar o deshabilitar rutas de acceso, establecer la directiva de múltiples rutas y especificar la ruta de acceso preferida.

Para obtener información sobre la administración de rutas de acceso, consulte Capítulo 18 Descripción de múltiples rutas y conmutación por error.

Las máquinas virtuales con RDM deben omitir la memoria caché de SCSI INQUIRY

Algunas máquinas virtuales con RDM deben obtener la información de SCSI INQUIRY desde el LUN en lugar de usar los datos de SCSI INQUIRY almacenados en la memoria caché mediante ESXi.

Problema

Ciertos sistemas operativos invitados o aplicaciones que se ejecutan en las máquinas virtuales con RDM muestran un comportamiento impredecible.

Causa

Este comportamiento podría deberse a que datos de SCSI INQUIRY almacenados en la memoria caché interfieren con sistemas operativos y aplicaciones invitados específicos.

Cuando el host ESXi se conecta por primera vez a un dispositivo de almacenamiento de destino, emite el comando SCSI INQUIRY para obtener datos de identificación básica desde el dispositivo. De forma predeterminada, ESXi almacena en la memoria caché los datos de SCSI INQUIRY que se reciben (Estándar, página 80 y página 83), y los datos permanecen sin modificaciones en adelante. Desde la memoria caché, se devuelven respuestas para los comandos de SCSI INQUIRY subsiguientes.

Sin embargo, los sistemas operativos invitados específicos que se ejecutan en máquinas virtuales con RDM deben consultar el LUN en lugar de usar los datos de SCSI INQUIRY almacenados en la memoria caché mediante ESXi. En estos casos, puede configurar la máquina virtual para que omita la memoria caché de SCSI INQUIRY.

Solución

◆ Utilice uno de los siguientes métodos.

Opción	Descripción
Modificar el archivo .vmx de la máquina virtual con RDM	Utilice este método para las máquinas virtuales con una versión de hardware 8 o posterior. a Agregue el siguiente parámetro al archivo: `scsix:y.ignoreDeviceInquiryCache = "true"` donde *x* es el número de controladora SCSI y *y* es el número de destino SCSI de RDM. b Reinicie la máquina virtual.
Usar el comando `esxcli`	Debido a que la opción se configura en un nivel de host, no se aplican limitaciones de versión de hardware de máquina virtual. `esxcli storage core device inquirycache set --device device id --ignore true` No se requiere reiniciar las máquinas virtuales.

Independientemente del método que utilice para establecer el parámetro de memoria caché de SCSI INQUIRY en true, la máquina virtual empieza a comunicarse con el LUN directamente en busca de los datos de SCSI INQUIRY.

Parámetro ignoreDeviceInquiryCache en vmx	Parámetro ignore inquirycache en esxcli	Solicitud de consulta procesada desde
True	True	LUN
False (valor predeterminado si el parámetro no está presente)	True	LUN
True	False	LUN
False (valor predeterminado si el parámetro no está presente)	False	Memoria caché

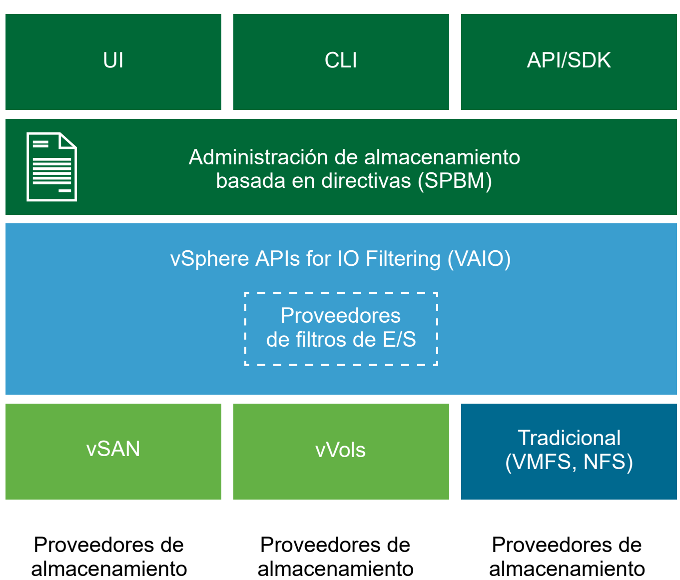
Administración de almacenamiento basada en directivas

20

En un centro de datos definido por software, la administración de almacenamiento basada en directivas (Storage Policy Based Management, SPBM) desempeña un papel importante, ya que permite alinear el almacenamiento con las demandas de aplicación de las máquinas virtuales. Proporciona un marco de directivas de almacenamiento que funciona como un panel de control unificado para un amplio rango de servicios de datos y soluciones de almacenamiento.

Como capa de abstracción, SPBM abstrae los servicios de almacenamiento ofrecidos por Virtual Volumes, vSAN, filtros de E/S u otras entidades de almacenamiento.

En lugar de integrarse con cada tipo individual de almacenamiento y servicio de datos, SPBM ofrece un marco universal para los diversos tipos de entidades de almacenamiento.



SPBM ofrece los siguientes mecanismos:

- Anuncio de las capacidades de almacenamiento y los servicios de datos que ofrecen las matrices de almacenamiento y otras entidades, como los filtros de E/S.
- Comunicaciones bidireccionales entre ESXi y vCenter Server, de un lado, y entre las matrices de almacenamiento y las entidades, del otro.
- Aprovisionamiento de máquinas virtuales basado en las directivas de almacenamiento de máquina virtual.

Este capítulo incluye los siguientes temas:

Directivas de almacenamiento de máquinas virtuales

Las directivas de almacenamiento de las máquinas virtuales son fundamentales para el aprovisionamiento de máquinas virtuales a través de SPBM. Las directivas controlan qué tipo de almacenamiento se proporciona para la máquina virtual y cómo esta se coloca en el almacenamiento. También determinan los servicios de datos que puede usar la máquina virtual.

vSphere ofrece directivas de almacenamiento predeterminadas. Además, puede definir directivas y asignarlas a las máquinas virtuales.

Puede utilizar la interfaz de directivas de almacenamiento de máquina virtual para crear una directiva de almacenamiento. Cuando defina la directiva, deberá especificar diversos requisitos de almacenamiento para las aplicaciones que se ejecutan en las máquinas virtuales. También se pueden utilizar las directivas de almacenamiento para solicitar servicios de datos específicos para los discos virtuales, como el almacenamiento en caché o la replicación.

La directiva de almacenamiento se aplica al crear, clonar o migrar la máquina virtual. Después de aplicar la directiva de almacenamiento, el mecanismo de SPBM lo asiste al colocar la máquina virtual en un almacén de datos coincidente. En algunos entornos de almacenamiento, el SPBM determina cómo los objetos de almacenamiento de máquinas virtuales se aprovisionan y se asignan dentro del recurso de almacenamiento para garantizar el nivel de servicio requerido. El SPBM también habilita los servicios de datos requeridos para la máquina virtual y lo ayuda a supervisar el cumplimiento de la directiva.

Flujo de trabajo de las directivas de almacenamiento de máquina virtual

El proceso completo de creación y administración de directivas de almacenamiento generalmente incluye varios pasos.

Según el tipo de servicios de datos o almacenamiento que ofrezca el entorno, es posible que deba realizar algún paso específico.

Paso	Descripción
Rellene la interfaz de directivas de almacenamiento de máquina virtual con los datos correspondientes.	La interfaz de directivas de almacenamiento de máquina virtual se rellena con la información sobre los almacenes de datos y los servicios de datos disponibles en el entorno de almacenamiento. Esta información se obtiene a través de los proveedores de almacenamiento y las etiquetas de almacén de datos. ■ Para las entidades representadas por proveedores de almacenamiento, compruebe que haya un proveedor adecuado registrado. Las entidades que utilizan el proveedor de almacenamiento son vSAN, Virtual Volumes y los filtros de E/S. En función del tipo de entidad de almacenamiento, algunos proveedores se registran automáticamente. Otros proveedores deben registrarse de forma manual. Consulte Utilizar proveedores de almacenamiento para rellenar la interfaz de directivas de almacenamiento de máquina virtual y Registrar proveedores de almacenamiento de Virtual Volumes. ■ Aplique etiquetas a los almacenes de datos no representados por los proveedores de almacenamiento. También se pueden utilizar etiquetas para indicar una propiedad no comunicada a través del proveedor de almacenamiento, como la ubicación geográfica o el grupo administrativo. Consulte Asignar etiquetas a almacenes de datos.
Cree componentes de directiva de almacenamiento predefinidos.	Un componente de directiva de almacenamiento describe un solo servicio de datos, como la replicación, que debe proporcionarse para la máquina virtual. Puede definir el componente con anticipación y asociarlo con varias directivas de almacenamiento de máquina virtual. Los componentes se pueden reutilizar e intercambiar. Consulte Crear componentes de directiva de almacenamiento.
Cree directivas de almacenamiento de máquina virtual.	Cuando define directivas de almacenamiento para máquinas virtuales, debe especificar los requisitos de almacenamiento para las aplicaciones que se ejecutan en las máquinas virtuales. Consulte Crear y administrar directivas de almacenamiento de máquina virtual.
Aplique la directiva de almacenamiento de máquina virtual a la máquina virtual.	Puede aplicar la directiva de almacenamiento al implementar la máquina virtual o configurar sus discos virtuales. Consulte Asignar directivas de almacenamiento a máquinas virtuales.
Compruebe el cumplimiento de la directiva de almacenamiento de máquina virtual.	Compruebe que la máquina virtual utilice el almacén de datos que cumple con la directiva de almacenamiento asignada. Consulte Comprobar el cumplimiento de una directiva de almacenamiento de máquina virtual.

Para crear y administrar las directivas de almacenamiento, utilice la interfaz Directiva de almacenamiento de máquina virtual de vSphere Client.

Rellenado de la interfaz de directivas de almacenamiento de máquina virtual

Antes de comenzar a crear directivas de almacenamiento de máquina virtual, debe rellenar la interfaz Directiva de almacenamiento de máquina virtual con información acerca de las entidades de almacenamiento y los servicios de datos disponibles en el entorno de almacenamiento.

Esta información se obtiene de los proveedores de almacenamiento, también denominados proveedores VASA. Otra fuente son las etiquetas del almacén de datos.

Servicios y capacidades de almacenamiento

Algunos almacenes de datos, como Virtual Volumes y vSAN, son representados por los proveedores de almacenamiento. A través de los proveedores de almacenamiento, los almacenes de datos publican sus capacidades en la interfaz de directivas de almacenamiento de máquina virtual. Estas capacidades de los almacenes de datos, los servicios de datos y otras características con rangos de valores rellenan la interfaz Directiva de almacenamiento de máquina virtual.

Puede utilizar estas características para definir reglas de servicio y colocación basadas en almacenes de datos para la directiva de almacenamiento.

Servicios de datos

Los proveedores de almacenamiento también representan filtros de E/S en los hosts. El proveedor de almacenamiento brinda información sobre los servicios de datos de los filtros a la interfaz Directiva de almacenamiento de máquina virtual. Utilice esta información al definir las reglas para los servicios de datos basados en host, también denominados “reglas comunes”. A diferencia de las reglas específicas de los almacenes de datos, las reglas comunes no definen la colocación de almacenamiento ni los requisitos de almacenamiento de la máquina virtual. En cambio, activan los servicios de datos de filtro de E/S solicitados para la máquina virtual.

Etiquetas

Por lo general, los almacenes de datos de VMFS y NFS no están representados por un proveedor de almacenamiento. Estos no muestran sus capacidades ni sus servicios de datos en la interfaz de directivas de almacenamiento de máquina virtual. Se pueden utilizar etiquetas para codificar información sobre estos almacenes de datos. Por ejemplo, puede etiquetar los almacenes de datos de VMFS como VMFS-Gold y VMFS-Silver para representar diferentes niveles de servicio.

En los almacenes de datos de Virtual Volumes y vSAN, puede utilizar etiquetas para codificar información no publicada por el proveedor de almacenamiento, como la ubicación geográfica (Palo Alto) o el grupo administrativo (Contabilidad).

Tal como ocurre con las capacidades y las características del almacenamiento, todas las etiquetas asociadas con los almacenes de datos aparecen en la interfaz de directivas de almacenamiento de máquina virtual. Puede utilizar las etiquetas al definir las reglas de selección de ubicación basadas en etiquetas.

Utilizar proveedores de almacenamiento para rellenar la interfaz de directivas de almacenamiento de máquina virtual

Para las entidades representadas por proveedores de almacenamiento (VASA), compruebe que haya un proveedor adecuado registrado. Una vez que los proveedores de almacenamiento

están registrados, la interfaz de directivas de almacenamiento de máquina virtual se rellena con información sobre los almacenes y los servicios de datos que representan los proveedores.

Las entidades que utilizan el proveedor de almacenamiento son vSAN, Virtual Volumes y los filtros de E/S. En función del tipo de entidad, algunos proveedores se registran automáticamente. Otros proveedores, como el proveedor de almacenamiento de Virtual Volumes, deben registrarse manualmente. Una vez que están registrados, los proveedores de almacenamiento aportan los siguientes datos a la interfaz de directivas de almacenamiento de máquina virtual:

- Capacidades y funciones de almacenamiento para almacenes de datos como Virtual Volumes y vSAN.
- Los servicios de datos que proporcionan los filtros de E/S.

Requisitos previos

Registre los proveedores de almacenamiento que requieran un registro manual. Para obtener más información, consulte la documentación correspondiente:

- *Administrar VMware vSAN*
- Capítulo 22 Trabajar con VMware vSphere Virtual Volumes
- Capítulo 23 Filtrar E/S de máquinas virtuales

Procedimiento

1. Desplácese hasta la instancia de vCenter Server.
2. Haga clic en la pestaña **Configurar** y, a continuación, en **Proveedores de almacenamiento**.
3. En la lista de proveedores de almacenamiento, vea los proveedores de almacenamiento registrados en vCenter Server.

   En la lista se muestra información general, como el nombre del proveedor de almacenamiento, su URL y estado, las entidades que representa el proveedor, etc.
4. Para ver más detalles, seleccione un proveedor de almacenamiento específico o su componente en la lista.

Asignar etiquetas a almacenes de datos

Puede usar etiquetas para codificar información acerca de un almacén de datos. Las etiquetas son útiles cuando el almacén de datos no está representado por un proveedor de almacenamiento ni anuncia sus capacidades y servicios en la interfaz de directivas de almacenamiento de máquina virtual. También puede usar las etiquetas para indicar una propiedad que no se comunica mediante un proveedor de almacenamiento, como una ubicación geográfica o un grupo administrativo.

Puede aplicar una etiqueta nueva que contenga información de almacenamiento general a un almacén de datos. Para obtener información sobre las etiquetas y sus categorías y sobre cómo administrar las etiquetas, consulte la documentación de *Administrar vCenter Server y hosts*.

Requisitos previos

Privilegios necesarios:

- **Etiquetado de vSphere.Crear etiqueta de vSphere** en la instancia de vCenter Server raíz
- **Etiquetado de vSphere.Crear categoría de etiqueta de vSphere** en la instancia de vCenter Server raíz
- **Etiquetado de vSphere.Asignar o desasignar etiqueta de vSphere** en la instancia de vCenter Server raíz

Procedimiento

1 En vSphere Client, cree una categoría para las etiquetas de almacenamiento.

a En el menú Inicio, haga clic en **Etiquetas y atributos personalizados**.

b Haga clic en la pestaña **Etiquetas** y, a continuación, en **Categorías**.

c Haga clic en el icono **Agregar categoría**.

d Especifique las opciones de la categoría. Vea el ejemplo siguiente:

Propiedad de la categoría	Ejemplo
Nombre de la categoría	Ubicación de almacenamiento
Descripción	Categoría de etiquetas relacionada con la ubicación del almacenamiento
Etiquetas por objeto	**Muchas etiquetas**
Tipos de objeto que se pueden asociar	**Almacén de datos** y **Clúster de almacenes de datos**

e Haga clic en **Aceptar**.

2 Cree una etiqueta de almacenamiento.

a En la pestaña **Etiquetas**, haga clic en **Etiquetas**.

b Haga clic en el icono **Agregar etiqueta**.

c Especifique las propiedades para la etiqueta. Vea el ejemplo siguiente:

Propiedad de etiqueta	Ejemplo
Nombre	Texas
Descripción	Almacén de datos ubicado en Texas
Categoría	Ubicación de almacenamiento

d Haga clic en **Aceptar**.

3 Aplique la etiqueta al almacén de datos.

   a Desplácese hasta el almacén de datos.

   b Haga clic con el botón derecho en el almacén de datos y seleccione **Etiquetas y atributos personalizados > Asignar etiqueta**.

   c En la lista de etiquetas, seleccione una etiqueta adecuada, como Texas, en la categoría Ubicación de almacenamiento y haga clic en **Asignar**.

Resultados

La etiqueta nueva se asigna al almacén de datos y aparece en la pestaña **Resumen** del almacén de datos en el panel **Etiquetas**.

Pasos siguientes

Al crear una directiva de almacenamiento de máquina virtual, puede hacer referencia a la etiqueta para incluir el almacén de datos etiquetado en la lista de recursos de almacenamiento compatibles. Consulte Crear una directiva de almacenamiento de máquina virtual para la ubicación basada en etiquetas.

También puede excluir el almacén de datos etiquetado de la directiva de almacenamiento de máquina virtual. Por ejemplo, su directiva de almacenamiento de máquina virtual puede incluir almacenes de datos de Virtual Volumes ubicados en Texas y California, pero excluir almacenes de datos ubicados en Nevada.

Para obtener más información sobre cómo se utilizan las etiquetas en las directivas de almacenamiento de máquinas virtuales, vea el siguiente vídeo.

(Usar etiquetas en directivas de almacenamiento)

Acerca de las reglas y los conjuntos de reglas

Después de rellenar la interfaz de las directivas de almacenamiento de máquina virtual con los datos correspondientes, puede comenzar a crear sus directivas de almacenamiento. La creación de una directiva implica la definición de reglas específicas de ubicación de almacenamiento y reglas de configuración de servicios de datos.

Reglas

La regla es un elemento básico de la directiva de almacenamiento de máquinas virtuales. Cada regla individual es una declaración que describe un solo requisito para el almacenamiento de máquina virtual y los servicios de datos.

Conjuntos de reglas

Dentro de una directiva de almacenamiento, las reglas individuales se organizan en colecciones de reglas o conjuntos de reglas. Por lo general, los conjuntos de reglas pueden ser de una de las siguientes categorías: reglas para servicios basados en host y reglas específicas para almacenes de datos.

Conjuntos de reglas específicos para almacenes de datos

Cada conjunto de reglas debe incluir reglas de ubicación que describen los requisitos para los recursos del almacenamiento de máquina virtual. Todas las reglas de ubicación de un mismo conjunto representan una única entidad de almacenamiento. Estas reglas pueden basarse en etiquetas o capacidades de almacenamiento.

Adicionalmente, el conjunto de reglas específicas para almacenes de datos puede incluir componentes de directivas de almacenamiento o reglas opcionales que describen los servicios de datos que se proporcionarán para la máquina virtual. Por lo general, estas reglas solicitan servicios como almacenamiento en caché, replicación y otros servicios proporcionados por sistemas de almacenamiento.

Para definir la directiva de almacenamiento, se requiere un conjunto específico para almacenes de datos. Los conjuntos de reglas adicionales son opcionales. Una sola directiva puede usar varios conjuntos de reglas para definir parámetros de ubicación de almacenamiento alternativos, a menudo de diversos proveedores de almacenamiento.

Reglas de ubicación: basadas en capacidades

Las reglas de ubicación especifican un requisito de almacenamiento en particular para la máquina virtual y habilitan el almacenamiento SPBM para distinguir los almacenes de datos compatibles entre todos los almacenes de datos del inventario. Estas reglas también describen cómo los objetos de almacenamiento de máquinas virtuales se asignan dentro del almacén de datos para recibir el nivel de servicio requerido. Por ejemplo, las reglas pueden enumerar Virtual Volumes como destino y definir el objetivo de punto de recuperación (Recovery Point Objective, RPO) máximo para los objetos de Virtual Volumes.

Cuando aprovisiona la máquina virtual, estas reglas guían la decisión que toma el SPBM acerca de la ubicación de la máquina virtual. El SPBM encuentra los almacenes de datos de Virtual Volumes que pueden coincidir con las reglas y satisfacer los requisitos de almacenamiento de la máquina virtual. Consulte Crear una directiva de almacenamiento de máquina virtual para Virtual Volumes.

Reglas de ubicación: basadas en etiquetas

Las reglas basadas en etiquetas hacen referencia a las etiquetas del almacén de datos. Estas reglas pueden definir la ubicación de la máquina virtual (por ejemplo, solicitar como destino todos los almacenes de datos con la etiqueta VMFS-Gold). También puede usar las reglas basadas en etiquetas para ajustar aún más la solicitud de ubicación de la máquina virtual. Por ejemplo, puede excluir los almacenes de datos con la etiqueta Palo Alto de la lista de almacenes de datos de Virtual Volumes. Consulte Crear una directiva de almacenamiento de máquina virtual para la ubicación basada en etiquetas.

Reglas para los servicios basados en host

Este conjunto de reglas activa los servicios de datos proporcionados por el host. El conjunto para los servicios basados en host puede incluir reglas o componentes de directiva de almacenamiento que describen servicios de datos específicos, como el cifrado o la replicación.

A diferencia de las reglas específicas para almacenes de datos, este conjunto no incluye reglas de ubicación. Las reglas para servicios basados en host son genéricas para todos los tipos de almacenamiento y no dependen del almacén de datos. Consulte Crear una directiva de almacenamiento de máquina virtual para los servicios de datos basados en host.

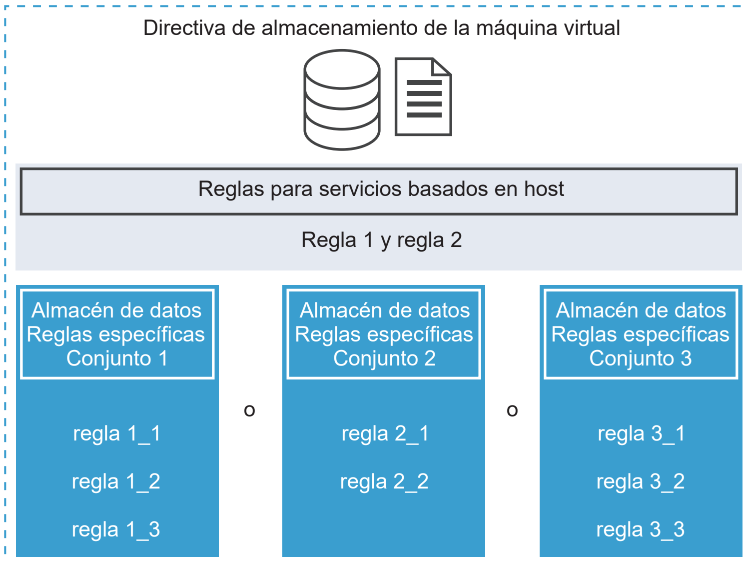
Tabla 20-1. Estructura de una directiva de almacenamiento de máquina virtual

Reglas para los servicios basados en host	Conjuntos de reglas específicos para almacenes de datos
Reglas o componentes de directivas de almacenamiento predefinidos para activar servicios de datos instalados en hosts ESXi. Por ejemplo, replicación mediante filtros de E/S.	Las reglas de ubicación basadas en capacidades o etiquetas que describen los requisitos de los recursos de almacenamiento de máquinas virtuales. Por ejemplo, colocación de Virtual Volumes.
	Reglas o componentes de directivas de almacenamiento predefinidos que activan los servicios de datos proporcionados por el almacenamiento. Por ejemplo, el almacenamiento en caché realizado por Virtual Volumes.

Relaciones entre reglas y conjuntos de reglas

El operador booleano `OR` define la relación entre los conjuntos de reglas específicos para almacenes de datos en la directiva. El operador `AND` define la relación entre todas las reglas dentro de un solo conjunto de reglas. La directiva puede contener únicamente un conjunto de reglas para servicios basados en host, un conjunto de reglas específico para almacenes de datos o ambos.

Si el conjunto de reglas para los servicios basados en hosts no está disponible, basta con seguir todas las reglas de un conjunto de reglas específico para almacenes de datos para cumplir con toda la directiva. Si el conjunto de reglas para los servicios basados en hosts está disponible, la directiva coincide con el almacén de datos que cumple con las reglas de servicios de host y con todas las reglas en uno de los conjuntos específicos para almacenes de datos.



Crear y administrar directivas de almacenamiento de máquina virtual

Para crear y administrar directivas de almacenamiento de máquina virtual, puede utilizar la interfaz Directivas de almacenamiento de máquina virtual.

Crear una directiva de almacenamiento de máquina virtual para los servicios de datos basados en host

Para definir la directiva de almacenamiento de máquina virtual en vSphere Client, utilice al asistente **Crear directiva de almacenamiento de máquina virtual**. En esta tarea, se crean reglas para los servicios de datos que ofrecen los hosts ESXi. La directiva de almacenamiento de máquina virtual que incluye estas reglas activa los servicios de datos especificados para la máquina virtual.

Los servicios de datos disponibles incluyen el cifrado, el control de E/S, el almacenamiento en caché y otros. Algunos servicios de datos, como el cifrado, los proporciona VMware. Se pueden obtener otros mediante los filtros de E/S de terceros que se instalen en el host.

Normalmente, los servicios de datos son genéricos para todos los tipos de almacenamiento y no dependen de un almacén de datos. La adición de reglas específicas de un almacén de datos a la directiva de almacenamiento es opcional.

Si agrega reglas específicas de un almacén de datos, y los dos filtros de E/S en el host y el almacenamiento ofrecen el mismo tipo de servicio (por ejemplo, el cifrado), la directiva puede solicitar este servicio a ambos proveedores. Como resultado, los datos de la máquina virtual se cifran dos veces, una mediante el filtro de E/S y otra mediante el almacenamiento. Sin embargo, la replicación proporcionada por Virtual Volumes y la replicación proporcionada por el filtro de E/S no pueden coexistir en la misma directiva de almacenamiento.

Requisitos previos

- Para obtener información sobre el cifrado de máquinas virtuales, consulte la documentación de *Seguridad de vSphere*.
- Para obtener información sobre los filtros de E/S, consulte Capítulo 23 Filtrar E/S de máquinas virtuales.
- Para obtener información sobre los componentes de directiva de almacenamiento, consulte Acerca de los componentes de directiva de almacenamiento.
- Privilegios necesarios: **Directivas de almacenamiento de máquina virtual.Actualizar** y **Directivas de almacenamiento de máquina virtual.Ver**.

Procedimiento

1 Abra al asistente **Crear directiva de almacenamiento de máquina virtual**.

   a Haga clic en **Menú > Directivas y perfiles**.

   b En **Directivas y perfiles**, haga clic en **Directivas de almacenamiento de máquina virtual**.

   c Haga clic en **Crear**.

2 Introduzca el nombre y la descripción de la directiva, y haga clic en **Siguiente**.

Opción	Acción
vCenter Server	Seleccione la instancia de vCenter Server.
Nombre	Introduzca el nombre de la directiva de almacenamiento.
Descripción	Introduzca la descripción de la directiva de almacenamiento.

3 En la página **Estructura de directiva** de **Servicios basados en hosts**, habilite las reglas basadas en hosts.

4 En la página **Servicios basados en hosts**, defina las reglas para habilitar y configurar los servicios de datos proporcionados por el host.

   a Haga clic en la pestaña de la categoría de servicio de datos, por ejemplo, **Replicación**.

   b Defina reglas personalizadas para la categoría de servicio de datos o utilice componentes predefinidos.

Opción	Descripción
Deshabilitado	Los servicios basados en hosts están deshabilitados de forma predeterminada.
Usar componente de directiva de almacenamiento	Seleccione un componente de directiva de almacenamiento en el menú desplegable. Esta opción solo está disponible si existen componentes predefinidos en la base de datos.
Personalizado	Si desea definir reglas personalizadas para la categoría de servicio de datos, especifique un proveedor adecuado y los valores de las reglas.

Nota Puede habilitar varios servicios de datos. Si utiliza el cifrado con otros servicios de datos, establezca el parámetro **Permitir filtros de E/S antes del cifrado** en **True** para que otros servicios, como la replicación, puedan analizar datos de texto no cifrado antes del cifrado.

5 En la página **Compatibilidad de almacenamiento**, revise la lista de almacenes de datos que coinciden con esta directiva.

   Para ser compatibles con la directiva de los servicios basados en hosts, los almacenes de datos deben estar conectados al host que proporciona estos servicios. Si agrega reglas específicas de un almacén de datos a la directiva, los almacenes de datos compatibles también deben cumplir con los requisitos de almacenamiento de la directiva.

6 En la página **Revisar y finalizar**, revise la configuración de la directiva de almacenamiento y haga clic en **Finalizar**.

   Para cambiar una configuración, haga clic en **Atrás** para volver a la página correspondiente.

Resultados

En la lista se mostrará la nueva directiva de almacenamiento de máquina virtual para los servicios de datos basados en hosts.

Crear una directiva de almacenamiento de máquina virtual para Virtual Volumes

Para definir la directiva de almacenamiento de máquina virtual en vSphere Client, utilice al asistente **Crear directiva de almacenamiento de máquina virtual**. En esta tarea, cree una directiva de almacenamiento personalizada compatible con Virtual Volumes. Al definir la directiva de almacenamiento de máquina virtual para Virtual Volumes, cree reglas destinadas a configurar los servicios de almacenamiento y de datos proporcionados por el almacén de datos de Virtual Volumes. Las reglas se aplican cuando la máquina virtual se coloca en el almacén de datos de

Virtual Volumes. La directiva de almacenamiento personalizada puede reemplazar a la directiva de almacenamiento predeterminada “Sin requisitos” de Virtual Volumes que proporciona VMware.

El procedimiento da por sentado que se está creando la directiva de almacenamiento de máquina virtual para Virtual Volumes. Para obtener información acerca de la directiva de almacenamiento de vSAN, consulte la documentación *Administrar VMware vSAN*.

Requisitos previos

- Compruebe que el proveedor de almacenamiento de Virtual Volumes esté disponible y activo. Consulte Registrar proveedores de almacenamiento de Virtual Volumes.
- Asegúrese de que la interfaz de directivas de almacenamiento de máquina virtual contenga la información sobre las entidades de almacenamiento y los servicios de datos disponibles en el entorno de almacenamiento. Consulte Rellenado de la interfaz de directivas de almacenamiento de máquina virtual.
- Defina los componentes adecuados de la directiva de almacenamiento. Consulte Crear componentes de directiva de almacenamiento.
- Privilegios necesarios: **Directivas de almacenamiento de máquina virtual.Actualizar** y **Directivas de almacenamiento de máquina virtual.Ver**.

Procedimiento

1 Abra al asistente **Crear directiva de almacenamiento de máquina virtual**.

   a Haga clic en **Menú > Directivas y perfiles**.

   b En **Directivas y perfiles**, haga clic en **Directivas de almacenamiento de máquina virtual**.

   c Haga clic en **Crear**.

2 Introduzca el nombre y la descripción de la directiva, y haga clic en **Siguiente**.

Opción	Acción
vCenter Server	Seleccione la instancia de vCenter Server.
Nombre	Introduzca el nombre de la directiva de almacenamiento, por ejemplo, Directiva de almacenamiento de Virtual Volumes.
Descripción	Introduzca la descripción de la directiva de almacenamiento.

3 En la página **Estructura de directiva** de Reglas específicas de almacenes de datos, habilite reglas para una entidad de almacenamiento de destino, por ejemplo, el almacenamiento de Virtual Volumes.

   Puede habilitar reglas para varios almacenes de datos. Varios conjuntos de reglas permiten que una sola directiva defina parámetros de ubicación de almacenamiento alternativos, con frecuencia de distintos proveedores de almacenamiento.

4 En la página de reglas de *Virtual Volumes*, defina las reglas de colocación de almacenamiento para el almacén de datos de Virtual Volumes de destino.

   a Haga clic en la pestaña **Colocación** y, a continuación, en **Agregar regla**.

   b En el menú desplegable Agregar regla, seleccione una capacidad disponible y especifique su valor.

      Por ejemplo, puede especificar la cantidad de operaciones de lectura por segundo para los objetos de Virtual Volumes.

      Puede incluir la cantidad de reglas que necesite para la entidad de almacenamiento seleccionada. Compruebe que los valores que proporciona se encuentren dentro del rango de valores que anuncia el almacén de datos de Virtual Volumes.

   c Para ajustar los detalles de la solicitud de colocación, haga clic en la pestaña **Etiquetas** y agregue una regla basada en etiquetas.

      Las reglas basadas en etiquetas pueden filtrar almacenes de datos mediante la inclusión o la exclusión de criterios de colocación específicos. Por ejemplo, su directiva de almacenamiento de máquina virtual puede incluir almacenes de datos de Virtual Volumes ubicados en Texas y California, pero excluir almacenes de datos ubicados en Nevada.

5 (opcional) Defina las reglas para configurar los servicios específicos de almacén de datos.

   Los servicios de datos, como el cifrado, el almacenamiento en caché o la replicación, los proporciona el almacenamiento. La directiva de almacenamiento de máquina virtual que hace referencia a los servicios de datos solicita estos servicios para la máquina virtual cuando esta se coloca en el almacén de datos de Virtual Volumes.

   a Haga clic en la pestaña de la categoría de servicio de datos, por ejemplo, **Replicación**.

   b Defina reglas personalizadas para la categoría de servicio de datos o utilice componentes predefinidos.

Opción	Descripción
Deshabilitado	Los servicios específicos del almacén de datos están deshabilitados de forma predeterminada.
Usar componente de directiva de almacenamiento	Seleccione un componente de directiva de almacenamiento en el menú desplegable. Esta opción solo está disponible si existen componentes predefinidos en la base de datos.
Personalizado	Si desea definir reglas personalizadas para la categoría de servicio de datos, especifique un proveedor adecuado y los valores de las reglas.

6 En la página **Compatibilidad de almacenamiento**, revise la lista de almacenes de datos que coinciden con esta directiva.

   Si la directiva incluye varios conjuntos de reglas, el almacén de datos debe cumplir con al menos un conjunto de reglas y con todas las reglas dentro de ese conjunto.

7 En la página **Revisar y finalizar**, revise la configuración de la directiva de almacenamiento y haga clic en **Finalizar**.

Para cambiar una configuración, haga clic en **Atrás** para volver a la página correspondiente.

Resultados

La nueva directiva de almacenamiento de máquina virtual compatible con Virtual Volumes aparecerá en la lista.

Pasos siguientes

Ahora es posible asociar esta directiva con una máquina virtual o designarla como predeterminada.

Crear una directiva de almacenamiento de máquina virtual para la ubicación basada en etiquetas

Las reglas basadas en etiquetas hacen referencia a las etiquetas que asigna a los almacenes de datos y puede filtrar los almacenes de datos que se utilizará para la colocación de las máquinas virtuales. Para definir la ubicación basada en etiquetas en vSphere Client, utilice el asistente **Crear directiva de almacenamiento de máquina virtual**.

Requisitos previos

- Asegúrese de que la interfaz de directivas de almacenamiento de máquina virtual contenga la información sobre las entidades de almacenamiento y los servicios de datos disponibles en el entorno de almacenamiento. Consulte Rellenado de la interfaz de directivas de almacenamiento de máquina virtual.
- Privilegios necesarios: **Directivas de almacenamiento de máquina virtual.Actualizar** y **Directivas de almacenamiento de máquina virtual.Ver**.

Procedimiento

1 Abra al asistente **Crear directiva de almacenamiento de máquina virtual**.

   a Haga clic en **Menú > Directivas y perfiles**.

   b En **Directivas y perfiles**, haga clic en **Directivas de almacenamiento de máquina virtual**.

   c Haga clic en **Crear**.

2 Introduzca el nombre y la descripción de la directiva, y haga clic en **Siguiente**.

Opción	Acción
vCenter Server	Seleccione la instancia de vCenter Server.
Nombre	Introduzca el nombre de la directiva de almacenamiento.
Descripción	Introduzca la descripción de la directiva de almacenamiento.

3 En la página **Estructura de directiva** en Reglas específicas del almacén de datos, habilite las reglas de ubicación basadas en etiquetas.

4 En la página **Colocación basada en etiquetas**, cree las reglas de la etiqueta.

   a Haga clic en **Agregar regla de etiqueta** y defina los criterios de colocación basada en etiquetas. Utilice lo siguiente como ejemplo.

Opción	Ejemplo
Categoría de etiqueta	Nivel de servicio
Opción de uso	Usar almacenamiento etiquetado como
Etiquetas	Oro

   Todos los almacenes de datos con la etiqueta Gold se tornan compatibles como el destino de la ubicación de almacenamiento.

   b (opcional) Agregue más reglas basadas en etiquetas.

5 En la página **Compatibilidad de almacenamiento**, revise la lista de almacenes de datos que coinciden con esta directiva.

6 En la página **Revisar y finalizar**, revise la configuración de la directiva de almacenamiento y haga clic en **Finalizar**.

   Para cambiar una configuración, haga clic en **Atrás** para volver a la página correspondiente.

Resultados

La nueva directiva de almacenamiento de máquina virtual compatible con almacenes de datos con etiqueta aparecerá en la lista.

Editar o clonar una directiva de almacenamiento de máquina virtual

Si cambian los requisitos de almacenamiento de las máquinas virtuales y los discos virtuales, se puede modificar la directiva de almacenamiento existente. También se puede crear una copia de una directiva de almacenamiento de máquina virtual existente mediante su clonación. Durante la clonación, se puede seleccionar la personalización de la directiva de almacenamiento original.

Requisitos previos

Privilegio necesario: **StorageProfile.View**

Procedimiento

1 En vSphere Client, desplácese a la directiva de almacenamiento.

   a Haga clic en **Menú > Directivas y perfiles**.

   b En **Directivas y perfiles**, haga clic en **Directivas de almacenamiento de máquina virtual**.

2 Seleccione la directiva de almacenamiento y haga clic en uno de los iconos siguientes:

   - **Editar**

- **Clonar**

3 (opcional) Modifique la directiva y haga clic en **Aceptar**.

4 Si edita la directiva de almacenamiento que utiliza una máquina virtual, vuelva a aplicar la directiva a la máquina virtual.

Opción	Descripción
Manualmente más adelante	Si selecciona esta opción, el estado de cumplimiento de todos los discos virtuales y los objetos de inicio de máquina virtual asociados con la directiva de almacenamiento cambia a Desactualizado. Para actualizar la configuración y el cumplimiento, vuelva a aplicar manualmente la directiva de almacenamiento a todas las entidades asociadas. Consulte Volver a aplicar una directiva de almacenamiento de máquinas virtuales.
Ahora	Actualice el estado de cumplimiento y de la máquina virtual inmediatamente después de editar la directiva de almacenamiento.

Acerca de los componentes de directiva de almacenamiento

Una directiva de almacenamiento de máquina virtual puede incluir uno o varios bloques de creación reutilizables e intercambiables, llamados componentes de directiva de almacenamiento. Cada componente describe un servicio de datos en particular que se proporcionará para la máquina virtual. Puede definir los componentes de la directiva con anticipación y asociarlos con varias directivas de almacenamiento de máquina virtual.

No puede asignar el componente predefinido directamente a una máquina virtual o a un disco virtual. En cambio, debe agregar el componente a la directiva de almacenamiento de máquina virtual y asignar la directiva a la máquina virtual.

El componente describe un tipo de servicio de un proveedor de servicio. Los servicios pueden variar según los proveedores que use, pero, en general, pertenecen a una de las siguientes categorías.

- Compresión
- Almacenamiento en caché
- Cifrado
- Replicación

Cuando crea un componente de directiva de almacenamiento, define las reglas para un tipo y grado de servicio específico.

El siguiente ejemplo muestra que las máquinas virtuales VM1 y VM2 tienen requisitos de ubicación idénticos, pero deben tener diferentes grados de servicios de replicación. Puede crear los componentes de directiva de almacenamiento con diferentes parámetros de replicación y agregar estos componentes a las directivas de almacenamiento relacionadas.

Tabla 20-2. Componentes de directivas de almacenamiento

Máquina virtual	Reglas de colocación	Componente de directiva de almacenamiento
VM1 requiere replicación cada 2 horas	Almacén de datos de Virtual Volumes	Replicación cada 2 horas
VM2 requiere replicación cada 4 horas	Almacén de datos de Virtual Volumes	Replicación cada 4 horas

El proveedor del servicio puede ser un sistema de almacenamiento, un filtro de E/S u otra entidad. Si el componente hace referencia a un filtro de E/S, se agrega al conjunto de reglas basadas en host de la directiva de almacenamiento. Los componentes que hacen referencia a entidades que no son filtros de E/S, por ejemplo, un sistema de almacenamiento, se agregan a conjuntos de reglas específicos del almacén de datos.

Cuando trabaje con los componentes, siga estas directrices:

- Cada componente puede incluir solo un conjunto de reglas. Todas las características de este conjunto de reglas pertenecen a un solo proveedor de los servicios de datos.
- Si se hace referencia al componente en la directiva de almacenamiento de máquina virtual, no puede eliminarlo. Antes de eliminar el componente, debe quitarlo de la directiva de almacenamiento o eliminar la directiva de almacenamiento.
- Cuando agrega componentes a la directiva, puede usar solo un componente de la misma categoría, por ejemplo, almacenamiento en caché, por conjunto de reglas.

Crear componentes de directiva de almacenamiento

Un componente de directiva de almacenamiento describe un solo servicio de datos, como la replicación, que debe proporcionarse para la máquina virtual. Puede definir el componente con anticipación y asociarlo con varias directivas de almacenamiento de máquina virtual. Los componentes se pueden reutilizar e intercambiar.

Procedimiento

1. En vSphere Client, abra el cuadro de diálogo **Nuevo componente de directiva de almacenamiento**.
   a. Haga clic en **Menú > Directivas y perfiles**.
   b. En **Directivas y perfiles**, haga clic en **Componentes de directivas de almacenamiento**.
2. Haga clic en **Crear componente de directiva de almacenamiento**.
3. Seleccione la instancia de vCenter Server.
4. Introduzca el nombre, por ejemplo, Replicación de 4 horas, y una descripción para el componente de la directiva.

   Asegúrese de que el nombre no entre en conflicto con los nombres de otros componentes de directivas de almacenamiento.
5. Seleccione la categoría de servicio, por ejemplo **Replicación**.

6 Seleccione el proveedor de servicio.

7 Defina las reglas para la categoría seleccionada.

Por ejemplo, si configura una replicación de 4 horas, establezca el valor de objetivo de punto de recuperación (Recovery Point Objective, RPO) en 4.

Para el cifrado basado en filtros de E/S, establezca el parámetro **Permitir filtros de E/S antes del cifrado**. El cifrado proporcionado por el almacenamiento no requiere este parámetro.

Opción	Descripción
False (predeterminado)	No permite utilizar otros filtros de E/S antes del filtro de cifrado.
True	Permite utilizar otros filtros de E/S antes del filtro de cifrado. Otros filtros, como la replicación, pueden analizar datos de texto no cifrado antes del cifrado.

8 Haga clic en **Aceptar**.

Resultados

El nuevo componente aparece en la lista de componentes de la directiva de almacenamiento.

Pasos siguientes

Puede agregar el componente a la directiva de almacenamiento de máquina virtual. Si el servicio de datos al que hace referencia el componente se proporciona mediante los filtros de E/S, agregue el componente a las reglas basadas en hosts de la directiva de almacenamiento. Los componentes que hacen referencia a entidades que no son filtros de E/S, por ejemplo, un sistema de almacenamiento, se agregan a conjuntos de reglas específicos del almacén de datos.

Editar o clonar componentes de directiva de almacenamiento

Puede modificar los componentes de directiva de almacenamiento existentes. También puede clonar el componente existente para crear una copia de él.

Procedimiento

1 En vSphere Client, desplácese al componente de directiva de almacenamiento para editar o clonar.

   a Haga clic en **Menú > Directivas y perfiles**.

   b En **Directivas y perfiles**, haga clic en **Componentes de directivas de almacenamiento**.

2 Seleccione el componente y haga clic en uno de los iconos siguientes.

Opción	Descripción
Editar configuración	Al editar, no puede cambiar la categoría del servicio de datos ni el proveedor. Por ejemplo, si el componente original hace referencia a la replicación proporcionada por los filtros de E/S, esta configuración debe permanecer sin cambios.
Clon	Al clonar, puede personalizar cualquier configuración del componente original.

3 Modifique los valores correspondientes y haga clic en **Aceptar**.

4 Si una directiva de almacenamiento de máquina virtual que está asignada a una máquina virtual hace referencia al componente de directiva que desea editar, vuelva a aplicar la directiva de almacenamiento a la máquina virtual.

Elemento del menú	Descripción
Manualmente más adelante	Si selecciona esta opción, el estado de cumplimiento de todos los discos virtuales y los objetos de inicio de máquina virtual asociados con la directiva de almacenamiento cambia a Desactualizado. Para actualizar la configuración y el cumplimiento, vuelva a aplicar manualmente la directiva de almacenamiento a todas las entidades asociadas. Consulte Volver a aplicar una directiva de almacenamiento de máquinas virtuales.
Ahora	Actualice el estado de cumplimiento y de la máquina virtual inmediatamente después de editar la directiva de almacenamiento.

Directivas de almacenamiento y máquinas virtuales

Después de definir una directiva de almacenamiento de máquina virtual, puede aplicarla a una máquina virtual. La directiva de almacenamiento se aplica al aprovisionar la máquina virtual o configurar sus discos virtuales. Según el tipo y la configuración, la directiva puede servir para diferentes usos. La directiva puede seleccionar el almacén de datos adecuado para la máquina virtual y aplicar el nivel de servicio correspondiente. También puede habilitar servicios de datos específicos para la máquina virtual y sus discos.

Si no se especifica la directiva de almacenamiento, el sistema utilizará la directiva de almacenamiento predeterminada asociada con el almacén de datos. Si cambian los requisitos de almacenamiento de las aplicaciones en la máquina virtual, puede modificar la directiva de almacenamiento que se aplicó originalmente a la máquina virtual.

Asignar directivas de almacenamiento a máquinas virtuales

Es posible asignar una directiva de almacenamiento de máquina virtual en una implementación inicial de una máquina virtual o cuando realiza otras operaciones de máquina virtual, como la clonación o la migración.

Este tema describe cómo asignar la directiva de almacenamiento de máquina virtual cuando crea una máquina virtual. Para obtener información sobre otros métodos de implementación, incluidas la clonación, la implementación a partir de una plantilla, etc., consulte la documentación *Administrar máquinas virtuales de vSphere*.

Se puede aplicar la misma directiva de almacenamiento al archivo de configuración de máquina virtual y a todos los discos virtuales. Si los requisitos de almacenamiento para los discos virtuales y el archivo de configuración son diferentes, se pueden asociar distintas directivas de almacenamiento con el archivo de configuración de máquina virtual y los discos virtuales seleccionados.

Procedimiento

1 Inicie el proceso de aprovisionamiento de máquina virtual y siga los pasos adecuados.

2 Asigne la misma directiva de almacenamiento a todos los discos y archivos de máquina virtual.

   a En la página **Seleccionar almacenamiento**, seleccione una directiva de almacenamiento en el menú desplegable **Directiva de almacenamiento de máquina virtual**.

   De acuerdo con la configuración, la directiva de almacenamiento separa todos los almacenes de datos en conjuntos compatibles e incompatibles. Si la directiva hace referencia a servicios de datos que ofrece una entidad de almacenamiento específica, por ejemplo, Virtual Volumes, la lista compatible incluye almacenes de datos que representan solo ese tipo de almacenamiento.

   b Seleccione un almacén de datos adecuado de la lista de almacenes de datos compatibles.

   El almacén de datos se transforma en el recurso de almacenamiento de destino del archivo de configuración de la máquina virtual y de todos los discos virtuales.

   c Si utiliza el servicio de replicación con Virtual Volumes, especifique el grupo de replicación.

   Los grupos de replicación indican qué máquinas virtuales y discos virtuales deben replicarse juntos en un sitio de destino.

Opción	Descripción
Grupo de replicación preconfigurado	Grupos de replicación que se configuran por adelantado por el lado de almacenamiento. vCenter Server y ESXi detectan los grupos de replicación, pero no administran su ciclo de vida.
Grupo de replicación automático	Virtual Volumes crea un grupo de replicación y asigna todos los objetos de la máquina virtual a este grupo.

3 Cambie la directiva de almacenamiento de máquina virtual del disco virtual.

   Utilice esta opción si los requisitos de selección de almacenamiento son distintos para los discos virtuales. También puede utilizar esta opción para habilitar servicios de filtro de E/S, como el almacenamiento en caché y la replicación, para sus discos virtuales.

   a En la página **Personalizar hardware**, expanda el panel **Disco duro nuevo**.

   b En el menú desplegable **Directiva de almacenamiento de máquina virtual**, seleccione la directiva de almacenamiento para asignar al disco virtual.

   c (opcional) Cambie la ubicación de almacenamiento del disco virtual.

      Use esta opción para almacenar el disco virtual en un almacén de datos distinto del almacén de datos en el que reside el archivo de configuración de máquina virtual.

4 Complete el proceso de aprovisionamiento de máquina virtual.

Resultados

Una vez creada la máquina virtual, la pestaña **Resumen** muestra las directivas de almacenamiento asignadas y su estado de cumplimiento.

Pasos siguientes

Si los requisitos de selección de almacenamiento del archivo de configuración o los discos virtuales cambian, se puede modificar la asignación de la directiva virtual posteriormente.

Cambiar la asignación de directivas de almacenamiento para archivos y discos de máquinas virtuales

Si cambian los requisitos de almacenamiento para las aplicaciones en la máquina virtual, puede editar la directiva de almacenamiento que se aplicó originalmente a la máquina virtual.

Puede editar la directiva de almacenamiento de una máquina virtual encendida o apagada.

Cuando cambia la asignación de una directiva de almacenamiento de máquina virtual, puede aplicar la misma directiva de almacenamiento al archivo de configuración de la máquina virtual y a todos sus discos virtuales. También puede asociar distintas directivas de almacenamiento con el archivo de configuración de la máquina virtual y los discos virtuales. Se aplicarían diferentes directivas si, por ejemplo, los requisitos de almacenamiento para los discos virtuales y el archivo de configuración fuesen diferentes.

Procedimiento

1 En vSphere Client, desplácese hasta la máquina virtual.

   a Haga clic en **Menú > Directivas y perfiles**.

   b En **Directivas y perfiles**, haga clic en **Directivas de almacenamiento de máquina virtual**.

c Haga clic en la directiva de almacenamiento que desea cambiar y haga clic en **Cumplimiento de la máquina virtual**.

Puede ver la lista de máquinas virtuales que usan esta directiva de almacenamiento.

d Haga clic en la máquina virtual cuya directiva desee modificar.

2 Haga clic en la pestaña **Configurar** y en **Directivas**.

3 Haga clic en **Editar directivas de almacenamiento de máquina virtual**.

4 Especifique la directiva de almacenamiento de máquina virtual para la máquina virtual.

Opción	Acciones
Aplique la misma directiva de almacenamiento a todos los objetos de la máquina virtual.	Seleccione la directiva en el menú desplegable **Directiva de almacenamiento de máquina virtual**.
Aplique distintas directivas de almacenamiento al objeto de inicio de la máquina virtual y a los discos virtuales.	a Active la opción **Configurar por disco**. b Seleccione el objeto, por ejemplo, el objeto de inicio de máquina virtual. c En la columna Directiva de almacenamiento de máquina virtual, seleccione la directiva en el menú desplegable.

5 Si usa la directiva de Virtual Volumes con replicación, configure el grupo de replicación.

Los grupos de replicación indican qué máquinas virtuales y discos virtuales deben replicarse juntos en un sitio de destino.

Todos los objetos de almacenamiento de una máquina virtual deben pertenecer al mismo grupo de replicación. No se pueden asignar grupos de replicación diferentes a distintos objetos de almacenamiento de una máquina virtual.

6 Haga clic en **Aceptar** para guardar los cambios en la directiva de almacenamiento de máquina virtual.

Resultados

La directiva de almacenamiento se asigna a la máquina virtual y a sus discos.

Comprobar el cumplimiento de una directiva de almacenamiento de máquina virtual

Se puede comprobar si una máquina virtual utiliza un almacén de datos compatible con los requisitos de almacenamiento especificados en la directiva de almacenamiento de máquina virtual.

Requisitos previos

Compruebe que haya una directiva de almacenamiento asociada con la máquina virtual.

Procedimiento

1 En vSphere Client, desplácese hasta la máquina virtual.

2 Haga clic en la pestaña **Configurar** y en **Directivas**.

3 Haga clic en **Comprobar el cumplimiento de la directiva de almacenamiento de máquina virtual**.

El sistema verificará el cumplimiento.

4 Vea el estado de cumplimiento.

Estado de cumplimiento	Descripción
Conforme	El almacén de datos que utilizan la máquina virtual o el disco virtual tiene las capacidades de almacenamiento compatibles con los requisitos de la directiva.
No compatible	El almacén de datos que utilizan la máquina virtual o el disco virtual no tiene las capacidades de almacenamiento compatibles con los requisitos de la directiva. Es posible migrar los archivos de la máquina virtual y los discos virtuales a los almacenes de datos compatibles.
Desactualizado	El estado indica que se editó la directiva, pero los nuevos requisitos no se han comunicado al almacén de datos donde residen los objetos de la máquina virtual. Para comunicar los cambios, vuelva a aplicar la directiva a los objetos desactualizados.
No aplicable	Esta directiva de almacenamiento hace referencia a capacidades de almacenes de datos no compatibles con el almacén de datos en el que reside la máquina virtual.

Pasos siguientes

Si no puede lograr que un almacén de datos cumpla con los requisitos, migre los archivos o los discos virtuales a un almacén de datos compatible. Consulte Encontrar un recurso de almacenamiento compatible para máquinas virtuales no compatibles.

Si el estado es Desactualizado, vuelva a aplicar la directiva a los objetos. Consulte Volver a aplicar una directiva de almacenamiento de máquinas virtuales.

Encontrar un recurso de almacenamiento compatible para máquinas virtuales no compatibles

Determine qué almacén de datos es compatible con la directiva de almacenamiento que está asociada con la máquina virtual.

Ocasionalmente, una directiva de almacenamiento asignada a una máquina virtual puede tener el estado de incumplimiento. Este estado indica que la máquina virtual o sus discos utilizan almacenes de datos que son incompatibles con la directiva. En este caso, se pueden migrar los archivos y los discos virtuales de la máquina virtual a almacenes de datos compatibles.

Utilice esta tarea para determinar qué almacenes de datos satisfacen los requisitos de la directiva.

Procedimiento

1 Compruebe que la directiva de almacenamiento para la máquina virtual esté en estado No conforme.

   a En vSphere Client, desplácese hasta la máquina virtual.

   b Haga clic en la pestaña **Resumen**.

   El panel Cumplimiento de la directiva de almacenamiento de máquina virtual, en el panel Directivas de almacenamiento de máquina virtual, muestra el estado No conforme.

2 Desplácese hasta la directiva de almacenamiento No conforme.

   a Haga clic en **Menú > Directivas y perfiles**.

   b En **Directivas y perfiles**, haga clic en **Directivas de almacenamiento de máquina virtual**.

3 Se mostrará la lista de almacenes de datos compatibles para la directiva de almacenamiento No conforme.

   a Haga clic en la directiva de almacenamiento.

   b Haga clic en **Compatibilidad de almacenamiento**.

   Aparecerá una lista de almacenes de datos que coinciden con los requisitos de la directiva.

Pasos siguientes

Es posible migrar la máquina virtual o sus discos a uno de los almacenes de datos incluidos en la lista.

Volver a aplicar una directiva de almacenamiento de máquinas virtuales

Después de editar una directiva de almacenamiento que ya está asociada con un objeto de máquina virtual, la directiva se debe volver a aplicar. Al hacerlo, los nuevos requisitos de almacenamiento se comunican al almacén de datos donde reside el objeto de máquina virtual.

Requisitos previos

El estado de cumplimiento de una máquina virtual es Desactualizado. El estado indica que la directiva se editó, pero los nuevos requisitos no se han comunicado al almacén de datos.

Procedimiento

1 En vSphere Client, desplácese hasta la máquina virtual.

2 Haga clic en la pestaña **Configurar** y en **Directivas**.

3 Compruebe que el estado de cumplimiento sea Desactualizado.

4 Haga clic en **Volver a aplicar directiva de almacenamiento de máquina virtual**.

5 Compruebe el estado de cumplimiento.

Estado de cumplimiento	Descripción
Conforme	El almacén de datos que utilizan la máquina virtual o el disco virtual tiene las capacidades de almacenamiento que requiere la directiva.
No compatible	El almacén de datos cumple con los requisitos de almacenamiento especificados, pero actualmente no puede cumplir con la directiva de almacenamiento. Por ejemplo, el estado puede ser de no cumplimiento cuando los recursos físicos del almacén de datos no están disponibles. Puede hacer que el almacén de datos esté en cumplimiento realizando cambios en la configuración física del clúster de hosts. Por ejemplo, agregando hosts o discos al clúster. Si los recursos adicionales cumplen con la directiva de almacenamiento, el estado pasará a ser Cumplimiento. Si no puede lograr que un almacén de datos cumpla con los requisitos, migre los archivos o los discos virtuales a un almacén de datos compatible. Consulte Encontrar un recurso de almacenamiento compatible para máquinas virtuales no compatibles.
No aplicable	La directiva de almacenamiento hace referencia a las capacidades del almacén de datos no admitidas por el almacén de datos.

Directivas de almacenamiento predeterminadas

Al aprovisionar una máquina virtual en un almacén de datos, debe asignar a la máquina virtual una directiva de almacenamiento de máquina virtual compatible. Si no configura ni asigna la directiva de almacenamiento de manera explícita a la máquina virtual, el sistema utiliza la directiva de almacenamiento predeterminada.

Directiva de almacenamiento predeterminada proporcionada por VMware

La directiva de almacenamiento predeterminada genérica que proporciona ESXi se aplica a todos los almacenes de datos y no incluye reglas específicas para ningún tipo de almacenamiento.

Además, ESXi ofrece directivas de almacenamiento predeterminadas para almacenes de datos basados en objetos, vSAN o Virtual Volumes. Estas directivas garantizan la colocación óptima de los objetos de la máquina virtual dentro del almacenamiento basado en objetos.

Para obtener información sobre la directiva de almacenamiento predeterminada de Virtual Volumes, consulte Virtual Volumes y directivas de almacenamiento de máquina virtual.

Los almacenes de datos de VMFS y NFS no tienen directivas predeterminadas específicas y pueden usar la directiva predeterminada genérica o una directiva personalizada que usted defina.

Directivas de almacenamiento predeterminadas definidas por el usuario

Puede crear una directiva de almacenamiento de máquina virtual compatible con vSAN o con Virtual Volumes. Luego, puede designar esta directiva como predeterminada para los almacenes de datos de vSAN y Virtual Volumes. La directiva predeterminada definida por el usuario reemplaza a la directiva de almacenamiento predeterminada que proporciona VMware.

Cada almacén de datos de vSAN y Virtual Volumes puede tener una sola directiva predeterminada a la vez. No obstante, es posible crear una sola directiva de almacenamiento con varios conjuntos de reglas de colocación, de modo que la directiva coincida con varios almacenes de datos de vSAN y Virtual Volumes. Puede designar esta directiva como predeterminada para todos los almacenes de datos.

Cuando la directiva de almacenamiento de máquina virtual se convierta en la directiva predeterminada de un almacén de datos, no podrá eliminarla a menos que la separe del almacén de datos.

Cambiar la directiva de almacenamiento predeterminada de un almacén de datos

Para los almacenes de datos de Virtual Volumes y vSAN, VMware proporciona directivas de almacenamiento que se utilizan como predeterminadas durante el aprovisionamiento de la máquina virtual. Es posible cambiar la directiva de almacenamiento predeterminada para un almacén de datos de Virtual Volumes o vSAN seleccionado.

Nota No designe una directiva de almacenamiento con reglas de replicación como directiva de almacenamiento predeterminada. De lo contrario, la directiva no permite que se seleccionen grupos de replicación.

Requisitos previos

Cree una directiva de almacenamiento que sea compatible con Virtual Volumes o vSAN. Puede crear una directiva que coincida con ambos tipos de almacenamiento.

Procedimiento

1 En vSphere Client, desplácese al almacén de datos.
2 Haga clic en la pestaña **Configurar** y en **General**.
3 En el panel Directiva de almacenamiento predeterminada, haga clic en **Editar**.
4 En la lista de directivas de almacenamiento disponibles, seleccione una directiva para designarla como la predeterminada y haga clic en **Aceptar**.

Resultados

La directiva de almacenamiento seleccionada pasa a ser la directiva predeterminada para el almacén de datos. El sistema asigna esta directiva a los objetos de máquina virtual que se aprovisionan en el almacén de datos cuando no hay otra directiva seleccionada.

Usar proveedores de almacenamiento 21

Un proveedor de almacenamiento es un componente de software que ofrece VMware o que desarrolla un tercero a través del programa vSphere APIs for Storage Awareness (VASA). El proveedor de almacenamiento también puede denominarse proveedor VASA. Los proveedores de almacenamiento se integran con diversas entidades de almacenamiento que incluyen almacenamiento físico externo y abstracciones de almacenamiento, como vSAN y Virtual Volumes. Los proveedores de almacenamiento también pueden admitir soluciones de software, por ejemplo, filtros de E/S.

Este capítulo incluye los siguientes temas:

Acerca de los proveedores de almacenamiento

Generalmente, vCenter Server y ESXi usan proveedores de almacenamiento para obtener información sobre la configuración del almacenamiento, el estado y los servicios de datos de almacenamiento que se ofrecen en su entorno. Esta información aparece en vSphere Client. La información ayuda a tomar las decisiones adecuadas sobre la ubicación de las máquinas virtuales, a establecer requisitos de almacenamiento y a supervisar el entorno de almacenamiento.

Proveedores de almacenamiento de persistencia

Los proveedores de almacenamiento que administran matrices y abstracciones de almacenamiento se denominan proveedores de almacenamiento de persistencia. Los proveedores que admiten Virtual Volumes o vSAN pertenecen a esta categoría. Además del almacenamiento, los proveedores de persistencia pueden ofrecer otros servicios de datos, como el de replicación.

Proveedores de servicios de datos

Otra categoría de proveedores es la de los proveedores de almacenamiento de filtro de E/S, o proveedores de servicios de datos. Estos proveedores ofrecen servicios de datos que incluyen almacenamiento en caché basado en host, compresión y cifrado.

Ambos proveedores de servicios de datos y almacenamiento de persistencia pueden pertenecer a una de estas categorías.

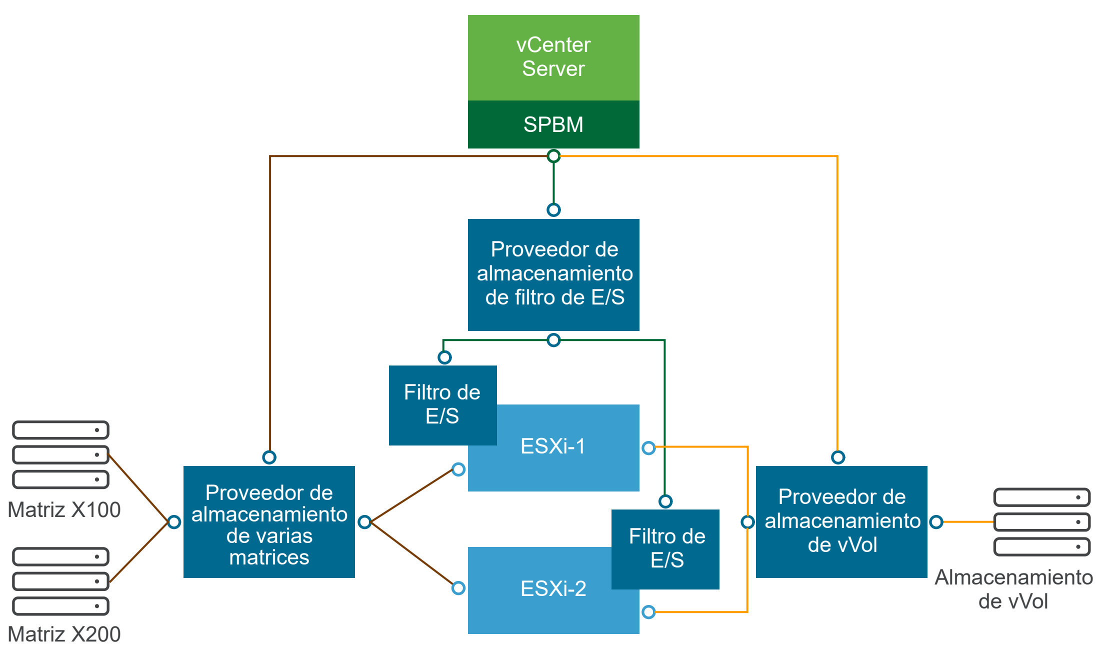
Proveedores de almacenamiento integrados

Proveedores de almacenamiento integrados proporcionados por VMware. Por lo general, no requieren registro. Por ejemplo, los proveedores de almacenamiento que admiten vSAN o filtros de E/S están integrados y se registran automáticamente.

Proveedores de almacenamiento de terceros

Cuando un tercero ofrece un proveedor de almacenamiento, en general es necesario registrar al proveedor. Un ejemplo es el proveedor de Virtual Volumes. Puede utilizar vSphere Client para registrar y administrar cada componente del proveedor de almacenamiento.

En el gráfico siguiente, se ilustra de qué manera los distintos tipos de proveedores de almacenamiento facilitan las comunicaciones entre vCenter Server y ESXi y otros componentes de su entorno de almacenamiento. Por ejemplo, entre estos componentes se incluyen las matrices de almacenamiento, almacenamiento de Virtual Volumes y filtros de E/S.



Proveedores de almacenamiento y representación de datos

vCenter Server y ESXi se comunican con el proveedor de almacenamiento para obtener información que este recopila del almacenamiento físico y definido por software subyacente, o desde los filtros de E/S disponibles. A continuación, vCenter Server puede mostrar los datos de almacenamiento en vSphere Client.

La información que proporciona el proveedor de almacenamiento puede dividirse en las siguientes categorías:

- Capacidades y servicios de datos de almacenamiento. Este tipo de información es esencial para funcionalidades como vSAN, Virtual Volumes y filtros de E/S. El proveedor de almacenamiento que representa estas funcionalidades se integra con el mecanismo de administración de almacenamiento basada en directivas (Storage Policy Based Management, SPBM). El proveedor de almacenamiento recopila información sobre servicios de datos que ofrecen entidades de almacenamiento subyacentes o filtros de E/S disponibles.

  Se hace referencia a estos servicios de datos cuando se definen los requisitos de almacenamiento para máquinas virtuales y discos virtuales en una directiva de almacenamiento. Según el entorno, el mecanismo de SPBM garantiza la ubicación adecuada del almacenamiento para una máquina virtual o habilita servicios de datos específicos para discos virtuales. Para obtener información detallada, consulte Crear y administrar directivas de almacenamiento de máquina virtual.

- Estado de almacenamiento. Esta categoría incluye informes sobre el estado de distintas entidades de almacenamiento. También incluye alarmas y eventos para notificar acerca de cambios de configuración.

  Este tipo de información puede ayudar a resolver problemas de rendimiento y conectividad de almacenamiento. También puede ser útil para facilitar la correlación de eventos y alarmas generados por la matriz con los correspondientes cambios de rendimiento y carga de esa matriz.

- Información de Storage DRS para la programación de recursos distribuidos en dispositivos de bloques o sistemas de archivos. Esta información ayuda a garantizar que las decisiones tomadas por Storage DRS sean compatibles con las decisiones de administración de recursos internas de los sistemas de almacenamiento.

Consideraciones y requisitos del proveedor de almacenamiento

Cuando se utilizan proveedores de almacenamiento de terceros, se aplican ciertos requisitos y consideraciones.

Generalmente, los proveedores son responsables de suministrar los proveedores de almacenamiento. El programa VMware VASA define una arquitectura que integra a los proveedores de almacenamiento de terceros en el entorno de vSphere, de modo que los hosts vCenter Server y ESXi puedan comunicarse con los proveedores de almacenamiento.

Para utilizar los proveedores de almacenamiento, cumpla estos requisitos:

- Asegúrese de que cada proveedor de almacenamiento esté certificado por VMware y correctamente implementado. Para obtener información sobre la implementación de proveedores de almacenamiento, póngase en contacto con el proveedor de almacenamiento.

- Asegúrese de que el proveedor de almacenamiento sea compatible con las versiones de vCenter Server y ESXi. Consulte *Guía de compatibilidad de VMware*.
- No instale el proveedor VASA en el mismo sistema que vCenter Server.
- Si el entorno contiene versiones anteriores de los proveedores de almacenamiento, pueden seguir utilizándose las funcionalidades existentes. No obstante, para usar las funciones nuevas, se debe actualizar el proveedor de almacenamiento a una versión más reciente.
- Cuando se actualiza un proveedor de almacenamiento a una versión posterior de VASA, debe cancelar el registro y volver a registrar el proveedor. Después del registro, vCenter Server puede detectar y usar la funcionalidad de la nueva versión de VASA.

Registrar proveedores de almacenamiento

Para establecer una conexión entre vCenter Server y un proveedor de almacenamiento, se debe registrar al proveedor de almacenamiento. Utilice vSphere Client para registrar un proveedor de almacenamiento distinto para cada host en un clúster.

Cuando se actualiza un proveedor de almacenamiento a una versión posterior de VASA, debe cancelar el registro y volver a registrar el proveedor. Una vez registrado, vCenter Server puede detectar y usar la funcionalidad de la versión más nueva de VASA.

Nota Si se utiliza vSAN, los proveedores de almacenamiento de vSAN se registran y aparecen en la lista de proveedores de almacenamiento automáticamente. vSAN no admite el registro manual de proveedores de almacenamiento. Consulte la documentación de *Administrar VMware vSAN*.

Requisitos previos

Compruebe que el componente del proveedor de almacenamiento esté instalado en el lado del almacenamiento y solicítele las credenciales correspondientes al administrador de almacenamiento.

Procedimiento

1. Desplácese hasta vCenter Server.
2. Haga clic en la pestaña **Configurar** y, a continuación, en **Proveedores de almacenamiento**.
3. Haga clic en el icono **Agregar**.
4. Introduzca la información de conexión del proveedor de almacenamiento, incluidos el nombre, la URL y las credenciales.

5 Especifique el método de seguridad.

Acción	Descripción
Dirigir vCenter Server al certificado del proveedor de almacenamiento	Seleccione la opción **Usar certificado de proveedor de almacenamiento** y especifique la ubicación del certificado.
Utilizar una huella digital del certificado del proveedor de almacenamiento	Si no guía a vCenter Server hasta el certificado del proveedor, se muestra la huella digital del certificado. Revise la huella digital y apruébela. vCenter Server agrega el certificado al almacén de confianza y procede con la conexión.

El proveedor de almacenamiento agrega el certificado de vCenter Server al almacén de confianza cuando vCenter Server se conecta por primera vez al proveedor.

6 Haga clic en **Aceptar**.

Resultados

vCenter Server registra el proveedor de almacenamiento y establece una conexión SSL segura con él.

Pasos siguientes

Para solucionar problemas de registro del proveedor de almacenamiento, consulte el artículo de la base de conocimientos de VMware https://kb.vmware.com/s/article/49798.

Ver información sobre el proveedor de almacenamiento

Después de registrar un componente del proveedor de almacenamiento en vCenter Server, aparece en la lista de proveedores de almacenamiento. Algunos proveedores de almacenamiento se registran automáticamente y aparecen en la lista después de que se configure la entidad que representan, por ejemplo, vSAN o filtros de E/S.

Utilice vSphere Client para ver la información general del proveedor de almacenamiento y los detalles de cada componente de almacenamiento.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en la pestaña **Configurar** y, a continuación, en **Proveedores de almacenamiento**.

3 En la lista de proveedores de almacenamiento, vea los proveedores de almacenamiento registrados en vCenter Server.

   En la lista se muestra información general, como el nombre del proveedor de almacenamiento, su URL y estado, la versión de las API de VASA, las entidades de almacenamiento que representa el proveedor, etc.

4 Para ver detalles adicionales, seleccione un proveedor de almacenamiento específico o su componente en la lista.

Nota Un único proveedor de almacenamiento puede admitir sistemas de almacenamiento de varios proveedores diferentes.

Administrar proveedores de almacenamiento

Utilice vSphere Client para realizar varias operaciones de administración en los proveedores de almacenamiento registrados.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en la pestaña **Configurar** y, a continuación, en **Proveedores de almacenamiento**.

3 Seleccione un proveedor de almacenamiento de la lista y haga clic en uno de los siguientes iconos.

Opción	Descripción
Sincronizar proveedores de almacenamiento	Sincronice todos los proveedores de almacenamiento con el estado actual del entorno.
Volver a examinar	Actualice los datos de almacenamiento del proveedor. vCenter Server actualiza periódicamente los datos de almacenamiento de su base de datos. Las actualizaciones son parciales y reflejan solo los cambios que los proveedores de almacenamiento comunican a vCenter Server en ese momento. Cuando sea necesario, puede realizar una sincronización total de la base de datos para el proveedor de almacenamiento seleccionado.
Quitar	Elimine del registro a los proveedores de almacenamiento que no utilice. Después de esta operación, vCenter Server finaliza la conexión y elimina al proveedor de almacenamiento de la configuración. **Nota** No puede cancelar manualmente el registro de ciertos proveedores de almacenamiento proporcionados por VMware, como los proveedores de almacenamiento de vSAN. Esta opción también es útil cuando se actualiza un proveedor de almacenamiento a una versión posterior de VASA. En este caso, debe eliminar del registro al proveedor y volver a registrarlo. Una vez registrado, vCenter Server puede detectar y usar la funcionalidad de la versión más nueva de VASA.
Actualizar certificado	vCenter Server advierte cuando un certificado asignado a un proveedor de almacenamiento está a punto de caducar. Puede actualizar el certificado para seguir utilizando ese proveedor. Si no se actualiza el certificado antes de que caduque, vCenter Server deja de utilizar el proveedor.

Resultados

vCenter Server finaliza la conexión y quita al proveedor de almacenamiento de la configuración.

Trabajar con VMware vSphere Virtual Volumes

22

VMware vSphere Virtual Volumes, también conocido como vVols, virtualiza los dispositivos de SAN y NAS mediante la extracción de recursos de hardware físico en grupos lógicos de capacidad. La funcionalidad de Virtual Volumes cambia el paradigma de administración de almacenamiento de la administración del espacio interno de los almacenes de datos a la administración de objetos de almacenamiento abstractos procesados por matrices de almacenamiento.

Este capítulo incluye los siguientes temas:

Acerca de Virtual Volumes

Con Virtual Volumes, una máquina virtual individual (no el almacén de datos) se convierte en una unidad de administración de almacenamiento, a la vez que el hardware de almacenamiento toma un control completo del contenido, del diseño y de la administración del disco virtual.

Históricamente, la administración de almacenamiento de vSphere se ha centrado en los almacenes de datos. Con este enfoque, los administradores de almacenamiento y los administradores de vSphere determinan de antemano los requisitos de almacenamiento de las máquinas virtuales. Posteriormente, el administrador de almacenamiento configura los recursos compartidos de LUN o NFS y los presenta a los hosts ESXi. El administrador de vSphere crea almacenes de datos basados en LUN o NFS, que luego usa como almacenamiento de máquinas virtuales. Generalmente, el almacén de datos es el nivel de granularidad más bajo en el que se produce la administración de datos desde el punto de vista del almacenamiento. Sin embargo, un solo almacén de datos contiene varias máquinas virtuales, que pueden tener diferentes requisitos. Con el enfoque tradicional, es difícil cumplir con los requisitos de una máquina virtual individual.

La funcionalidad de Virtual Volumes ayuda a mejorar la granularidad. Ayuda a diferenciar los servicios de la máquina virtual por aplicación al ofrecer un nuevo enfoque para la administración de almacenamiento. En lugar de determinar el almacenamiento de acuerdo con las características de un sistema de almacenamiento, Virtual Volumes lo hace en función de la necesidad de cada máquina virtual, lo que hace que el almacenamiento sea específico de cada máquina virtual.

Virtual Volumes asigna discos virtuales y sus derivados, clones, instantáneas y réplicas directamente a los objetos, llamados volúmenes virtuales, en un sistema de almacenamiento. Esta asignación permite que vSphere asigne operaciones de almacenamiento intensivas, como la creación de instantáneas, la clonación y la replicación, en el sistema de almacenamiento.

Al crear un volumen para cada disco virtual, es posible establecer directrices en un nivel óptimo. Puede decidir con anticipación cuáles son los requisitos de almacenamiento de una aplicación y comunicar estos requisitos al sistema de almacenamiento. El sistema de almacenamiento crea un disco virtual apropiado basado en estos requisitos. Por ejemplo, si la máquina virtual requiere una matriz de almacenamiento activo-activo, ya no es necesario que seleccione un almacén de datos que admita el modelo activo-activo. En cambio, puede crear un volumen virtual individual que se coloca automáticamente en la matriz de modelo activo-activo.

Conceptos de Virtual Volumes

Con Virtual Volumes, los contenedores de almacenamiento abstracto reemplazan a los volúmenes de almacenamiento tradicionales basados en recursos compartidos de NFS o LUN. En vCenter Server, los almacenes de datos de Virtual Volumes representan los contenedores de almacenamiento. Los almacenes de datos de Virtual Volumes almacenan volúmenes virtuales, objetos que encapsulan archivos de máquina virtual.

Mire el video para conocer más sobre los diferentes componentes de la funcionalidad Virtual Volumes.

(Virtual Volumes Parte 1: Conceptos)

- Objetos de Virtual Volumes

  Los volúmenes virtuales son encapsulaciones de archivos de máquinas virtuales, discos virtuales y sus derivados.

- Proveedores de almacenamiento de Virtual Volumes

  Un proveedor de almacenamiento de Virtual Volumes, también denominado proveedor VASA, es un componente de software que actúa como servicio de reconocimiento del almacenamiento de vSphere. El proveedor media la comunicación fuera de banda entre vCenter Server y los hosts ESXi, por un lado, y un sistema de almacenamiento, por el otro.

- Contenedores de almacenamiento de Virtual Volumes

  A diferencia del almacenamiento basado en LUN y NFS tradicional, la funcionalidad Virtual Volumes no requiere volúmenes configurados previamente en el lado del almacenamiento. En cambio, Virtual Volumes utiliza un contenedor de almacenamiento. Este contenedor es un grupo de capacidad de almacenamiento sin procesar o una adición de capacidades de almacenamiento que un sistema de almacenamiento puede proporcionar a los volúmenes virtuales.

- Extremos de protocolo

  A pesar de que los sistemas de almacenamiento administran todos los aspectos de los volúmenes virtuales, los hosts ESXi no tienen acceso directo a los volúmenes virtuales del lado del almacenamiento. En su lugar, los hosts ESXi usan un proxy de E/S lógico, denominado extremo de protocolo, para comunicarse con los volúmenes virtuales y los archivos de disco virtual que encapsulan los volúmenes virtuales. ESXi usa extremos de protocolo para establecer una ruta de acceso de datos a petición desde las máquinas virtuales a sus volúmenes virtuales respectivos.

- Enlazar y desenlazar volúmenes virtuales con extremos de protocolo

  En el momento de su creación, un volumen virtual es una entidad pasiva que no está lista inmediatamente para E/S. Para acceder al volumen virtual, ESXi o vCenter Server envían una solicitud de enlace.

- Almacenes de datos de Virtual Volumes

  Un almacén de datos de Virtual Volumes representa un contenedor de almacenamiento en vCenter Server y vSphere Client.

- Virtual Volumes y directivas de almacenamiento de máquina virtual

  Una máquina virtual que se ejecuta en un almacén de datos de Virtual Volumes necesita una directiva de almacenamiento de máquina virtual.

Objetos de Virtual Volumes

Los volúmenes virtuales son encapsulaciones de archivos de máquinas virtuales, discos virtuales y sus derivados.

Los volúmenes virtuales se almacenan de manera nativa en un sistema de almacenamiento que está conectado a los hosts ESXi a través de Ethernet o SAN. Un sistema de almacenamiento compatible los exporta como objetos y el hardware los administra completamente en el lado del almacenamiento. Por lo general, un GUID único identifica un volumen virtual. Los volúmenes

virtuales no se aprovisionan previamente, sino que se crean automáticamente al realizar operaciones de administración de máquinas virtuales. Entre estas operaciones se encuentran la creación y la clonación de máquinas virtuales, además de la creación de instantáneas. ESXi y vCenter Server asocian uno o varios volúmenes virtuales con una máquina virtual.

Tipos de Virtual Volumes

El sistema crea los siguientes tipos de volúmenes virtuales para los elementos principales que componen la máquina virtual:

Data-vVol

Un volumen virtual de datos que se corresponde directamente con el archivo `.vmdk` de cada disco virtual. Al igual que los archivos de discos virtuales en almacenes de datos tradicionales, los volúmenes virtuales se presentan como discos SCSI ante las máquinas virtuales. Data-vVol puede tener aprovisionamiento grueso o fino.

Config-vVol

Un volumen virtual de configuración, o un directorio de inicio, representa un pequeño directorio que contiene archivos de metadatos para una máquina virtual. Entre los archivos se encuentran un archivo `.vmx`, archivos de descriptores para discos virtuales, archivos de registro, etc. El volumen virtual de configuración está formateado con un sistema de archivos. Cuando ESXi utiliza el protocolo SCSI para conectarse al almacenamiento, los volúmenes virtuales de configuración se formatean con VMFS. Con el protocolo NFS, los volúmenes virtuales de configuración se presentan como un directorio NFS. Por lo general, es de aprovisionamiento fino.

Swap-vVol

Se crea la primera vez que se enciende una máquina virtual. Es un volumen virtual que contiene copias de páginas de memoria de máquina virtual que no pueden retenerse en la memoria. Su tamaño se determina según el tamaño de memoria de la máquina virtual. Es de aprovisionamiento grueso de forma predeterminada.

Snapshot-vVol

Un volumen de memoria virtual que incluye el contenido de la memoria de la máquina virtual para una snapshot. Con aprovisionamiento grueso.

Otro

Un volumen virtual para funciones específicas. Por ejemplo, se crea un volumen virtual de resumen para caché de lectura basada en contenido (Content-Based Read Cache, CBRC).

Generalmente, una máquina virtual crea un mínimo de tres volúmenes virtuales: data-vVol, config-vVol, y swap-vVol. El máximo depende de cuántos discos virtuales y snapshots residen en la máquina virtual.

Por ejemplo, el siguiente servidor SQL tiene seis volúmenes virtuales:

- Config-vVol
- Data-vVol para el sistema operativo
- Data-vVol para la base de datos
- Data-vVol para el registro
- Swap-vVol para el encendido
- Snapshot-vVol

Al utilizar diferentes volúmenes virtuales para distintos componentes de la máquina virtual, es posible aplicar y manipular directivas de almacenamiento en el nivel de granularidad más fino. Por ejemplo, un volumen virtual que contenga un disco virtual puede tener un conjunto más completo de servicios que el volumen virtual del disco de arranque de la máquina virtual. De manera similar, un volumen virtual de instantánea puede utilizar un nivel de almacenamiento diferente a comparación de un volumen virtual actual.

Aprovisionamiento de disco

La funcionalidad Virtual Volumes admite un concepto de discos virtuales con aprovisionamiento fino y grueso. Sin embargo, desde una prospectiva de E/S, la implementación y la administración de aprovisionamiento grueso o fino por parte de las matrices son transparentes para el host ESXi. ESXi no descarga en las matrices de almacenamiento ninguna de las funciones relacionadas con el aprovisionamiento fino. En la ruta de acceso de datos, ESXi no trata los volúmenes virtuales finos o gruesos de forma diferente.

Seleccione el disco virtual de formato fino o grueso en el momento de creación de la máquina virtual. Si el disco es de formato fino y reside en un almacén de datos de Virtual Volumes, no se puede expandir el disco para cambiar de tipo más adelante.

Discos compartidos

Puede colocar un disco compartido en un almacenamiento de Virtual Volumes compatible con las reservas de SCSI persistentes para Virtual Volumes. Puede utilizar este disco como un disco de cuórum y eliminar las RDM en los clústeres de MSCS. Para obtener más información, consulte la documentación sobre *Administrar recursos de vSphere*.

Proveedores de almacenamiento de Virtual Volumes

Un proveedor de almacenamiento de Virtual Volumes, también denominado proveedor VASA, es un componente de software que actúa como servicio de reconocimiento del almacenamiento de vSphere. El proveedor media la comunicación fuera de banda entre vCenter Server y los hosts ESXi, por un lado, y un sistema de almacenamiento, por el otro.

El proveedor de almacenamiento se implementa a través de VMware API for Storage Awareness (VASA) y se utiliza para administrar todos los aspectos de almacenamiento de Virtual Volumes. El proveedor de almacenamiento se integra con el servicio de supervisión de almacenamiento (SMS), proporcionado con vSphere, para comunicarse con vCenter Server y los hosts ESXi.

El proveedor de almacenamiento envía información desde el contenedor de almacenamiento subyacente. Las capacidades del contenedor de almacenamiento aparecen en vCenter Server y en vSphere Client. A continuación, a su vez, el proveedor de almacenamiento comunica los requisitos de almacenamiento de la máquina virtual, que se pueden definir en la forma de una directiva de almacenamiento, a la capa de almacenamiento. Este proceso de integración garantiza que un volumen virtual creado en la capa de almacenamiento cumpla con los requisitos detallados en la directiva.

Por lo general, los proveedores son los responsables de suministrar proveedores de almacenamiento que puedan integrarse con vSphere y admitir Virtual Volumes. Cada proveedor de almacenamiento debe tener certificación de VMware y estar correctamente implementado. Para obtener información acerca de la implementación y actualización de un proveedor de almacenamiento de Virtual Volumes a una versión compatible con la versión actual de ESXi, póngase en contacto con su proveedor de almacenamiento.

Una vez implementado el proveedor de almacenamiento, este se debe registrar en vCenter Server, para que pueda comunicarse con vSphere a través de SMS.

Contenedores de almacenamiento de Virtual Volumes

A diferencia del almacenamiento basado en LUN y NFS tradicional, la funcionalidad Virtual Volumes no requiere volúmenes configurados previamente en el lado del almacenamiento. En cambio, Virtual Volumes utiliza un contenedor de almacenamiento. Este contenedor es un grupo de capacidad de almacenamiento sin procesar o una adición de capacidades de almacenamiento que un sistema de almacenamiento puede proporcionar a los volúmenes virtuales.

Un contenedor de almacenamiento es parte del tejido de almacenamiento lógico y es una unidad lógica del hardware subyacente. El contenedor de almacenamiento agrupa de forma lógica los volúmenes virtuales según las necesidades de administración y gestión. Por ejemplo, el contenedor de almacenamiento puede contener todos los volúmenes virtuales creados para una empresa en una implementación multiempresa o un departamento en una implementación empresarial. Cada contenedor de almacenamiento funciona como un almacén de volúmenes virtuales, y los volúmenes virtuales se asignan de la capacidad del contenedor de almacenamiento.

Generalmente, un administrador de almacenamiento del lado del almacenamiento define los contenedores de almacenamiento. La cantidad de contenedores de almacenamiento, su capacidad y su tamaño dependen de la implementación específica del proveedor. Se requiere al menos un contenedor para cada sistema de almacenamiento.

Nota Un único contenedor de almacenamiento no puede expandir distintas matrices físicas.

Luego de registrar un proveedor de almacenamiento asociado con el sistema de almacenamiento, vCenter Server detecta todos los contenedores de almacenamiento configurados junto con sus perfiles de funcionalidad de almacenamiento, extremos de protocolo y demás atributos. Un único contenedor de almacenamiento puede exportar varios perfiles de funcionalidad. Como resultado, las máquinas virtuales con distintas necesidades y diferente configuración de directivas de almacenamiento pueden ser parte del mismo contenedor de almacenamiento.

Inicialmente, todos los contenedores de almacenamiento detectados no están conectados a ningún host específico, y no se los puede ver en vSphere Client. Para montar un contenedor de almacenamiento, debe asignarlo a un almacén de datos de Virtual Volumes.

Extremos de protocolo

A pesar de que los sistemas de almacenamiento administran todos los aspectos de los volúmenes virtuales, los hosts ESXi no tienen acceso directo a los volúmenes virtuales del lado del almacenamiento. En su lugar, los hosts ESXi usan un proxy de E/S lógico, denominado extremo de protocolo, para comunicarse con los volúmenes virtuales y los archivos de disco virtual que encapsulan los volúmenes virtuales. ESXi usa extremos de protocolo para establecer una ruta de acceso de datos a petición desde las máquinas virtuales a sus volúmenes virtuales respectivos.

Cada volumen virtual está enlazado a un extremo de protocolo específico. Cuando una máquina virtual en el host realiza una operación de E/S, el extremo de protocolo direcciona la E/S al volumen virtual adecuado. Normalmente, un sistema de almacenamiento requiere unos pocos extremos de protocolo. Un solo extremo de protocolo puede conectarse a cientos o miles de volúmenes virtuales.

Del lado del almacenamiento, el administrador de almacenamiento configura los extremos de protocolo, uno o varios por contenedor de almacenamiento. Los extremos de protocolo forman parte del tejido de almacenamiento físico. El sistema de almacenamiento exporta los extremos de protocolo con los contenedores de almacenamiento asociados a través de un proveedor de almacenamiento. Después de asignar el contenedor de almacenamiento a un almacén de datos de Virtual Volumes, el host ESXi detecta los puntos de acceso de protocolo, los cuales se muestran en vSphere Client. Los extremos de protocolo también se pueden detectar cuando se vuelve a examinar el almacenamiento. Varios hosts pueden detectar y montar los extremos de protocolo.

En vSphere Client, la lista de extremos de protocolo disponibles es similar a la lista de dispositivos de almacenamiento del host. Se pueden usar distintos transportes de almacenamiento para exponer los extremos de protocolo a ESXi. Cuando se usa el transporte basado en SCSI, el extremo de protocolo representa un LUN de proxy definido por un WWN de LUN basado en T10. Para el protocolo NFS, el endpoint de protocolo es un punto de montaje, como una dirección IP y un nombre del recurso compartido. Es posible configurar múltiples rutas en un extremo de protocolo basado en SCSI, pero no en un extremo de protocolo basado en NFS. Sin importar el protocolo que se utilice, la matriz de almacenamiento puede proporcionar varios extremos de protocolo para fines de disponibilidad.

Los extremos de protocolo se administran por matriz. ESXi y vCenter Server asumen que todos los extremos de protocolo notificados para una matriz se encuentran asociados a todos los contenedores de esa matriz. Por ejemplo, si una matriz tiene dos contenedores y tres extremos de protocolo, ESXi asume que se pueden enlazar los volúmenes virtuales de ambos contenedores a los tres extremos de protocolo.

Enlazar y desenlazar volúmenes virtuales con extremos de protocolo

En el momento de su creación, un volumen virtual es una entidad pasiva que no está lista inmediatamente para E/S. Para acceder al volumen virtual, ESXi o vCenter Server envían una solicitud de enlace.

El sistema de almacenamiento responde con un identificador de extremo de protocolo que se convierte en un punto de acceso al volumen virtual. El extremo de protocolo acepta todas las solicitudes de E/S hacia el volumen virtual. Este enlace existe hasta que ESXi envía una solicitud de desenlace para el volumen virtual.

Para solicitudes de enlace posteriores en el mismo volumen virtual, el sistema de almacenamiento puede devolver distintos identificadores de extremo de protocolo.

Al recibir solicitudes de enlace simultáneas hacia un volumen virtual de varios hosts ESXi, el sistema de almacenamiento puede devolver el mismo enlace de extremo o uno distinto a cada host ESXi solicitante. En otras palabras, el sistema de almacenamiento puede enlazar diferentes hosts simultáneos al mismo volumen virtual a través de extremos diferentes.

La operación de desenlace elimina el punto de acceso de E/S del volumen virtual. El sistema de almacenamiento puede desenlazar el volumen virtual de su extremo de protocolo de forma inmediata o después de un retraso, o bien realizar otra acción. Un volumen virtual enlazado no puede eliminarse sin desenlazarse previamente.

Almacenes de datos de Virtual Volumes

Un almacén de datos de Virtual Volumes representa un contenedor de almacenamiento en vCenter Server y vSphere Client.

Después de que vCenter Server detecta los contenedores de almacenamiento exportados por los sistemas de almacenamiento, es necesario montarlos como almacenes de datos de Virtual Volumes. Los almacenes de datos de Virtual Volumes no se formatean de la manera tradicional como, por ejemplo, almacenes de datos VMFS. Debe crearlos ya que todas las funcionalidades de vSphere, incluidas FT, HA, DRS, etc., requieren la construcción del almacén de datos para funcionar correctamente.

Puede utilizar el asistente de creación de almacén de datos en vSphere Client para asignar un contenedor de almacenamiento a un almacén de datos de Virtual Volumes. El almacén de datos de Virtual Volumes que crea corresponde directamente al contenedor de almacenamiento específico.

Desde una prospectiva de administrador de vSphere, el almacén de datos de Virtual Volumes es similar a cualquier otro almacén de datos y se usa para mantener máquinas virtuales. Como en los otros almacenes de datos, en el almacén de datos de Virtual Volumes se pueden buscar y enumerar los volúmenes virtuales por nombre de máquina virtual. Como en los almacenes de datos tradicionales, el almacén de datos de Virtual Volumes admite el montaje y el desmontaje. Sin embargo, las operaciones como la actualización y el cambio de tamaño no se aplican al almacén de datos de Virtual Volumes. El administrador de almacenamiento puede configurar la capacidad de almacén de datos de Virtual Volumes fuera de vSphere.

Los almacenes de datos de Virtual Volumes se pueden usar con almacenes de datos de VMFS y NFS tradicionales, y con vSAN.

Nota El tamaño de un volumen virtual debe ser un múltiplo de 1 MB y tener un tamaño mínimo de 1 MB. Como resultado, todos los discos virtuales que aprovisione en un almacén de datos de Virtual Volumes deben ser un múltiplo par de 1 MB. Si el disco virtual que se migra al almacén de datos de Virtual Volumes no tiene un múltiplo par de 1 MB, extienda el disco al múltiplo par de 1 MB más próximo.

Virtual Volumes y directivas de almacenamiento de máquina virtual

Una máquina virtual que se ejecuta en un almacén de datos de Virtual Volumes necesita una directiva de almacenamiento de máquina virtual.

Una directiva de almacenamiento de máquina virtual es un conjunto de reglas que contienen requisitos de calidad de servicio y selección de una máquina virtual. Esta directiva aplica una selección apropiada de la máquina virtual dentro del almacenamiento de Virtual Volumes y garantiza que el almacenamiento pueda satisfacer los requisitos de la máquina virtual.

Puede utilizar la interfaz de directivas de almacenamiento de máquina virtual para crear una directiva de almacenamiento de Virtual Volumes. Cuando asigna la directiva nueva a la máquina virtual, la directiva se encarga de que el almacenamiento de Virtual Volumes cumpla los requisitos.

Directiva de almacenamiento predeterminada de Virtual Volumes

Para Virtual Volumes, VMware proporciona una directiva de almacenamiento predeterminada que no contiene reglas ni requisitos de almacenamiento, denominada "directiva de sin requisitos de Virtual Volumes". Esta directiva se aplica a los objetos de máquina virtual cuando no se especifica otra directiva para la máquina virtual en el almacén de datos de Virtual Volumes. Con la directiva sin requisitos, las matrices de almacenamiento pueden determinar la selección óptima de los objetos de la máquina virtual.

La directiva sin requisitos predeterminada que proporciona VMware tiene las siguientes características:

- No puede eliminar, editar ni clonar esta directiva.
- La directiva es compatible solo con los almacenes de datos de Virtual Volumes.

- Puede crear una directiva de almacenamiento de máquina virtual para Virtual Volumes y designarla como predeterminada.

Protocolos de Virtual Volumes y almacenamiento

Un sistema de almacenamiento de Virtual Volumes proporciona extremos de protocolo que se pueden detectar en el tejido de almacenamiento físico. Los hosts ESXi usan los extremos de protocolo para conectarse a volúmenes virtuales en el almacenamiento. La operación de los extremos de protocolo depende de los protocolos de almacenamiento que exponen los endpoints en los hosts ESXi.

Virtual Volumes admite NFS versión 3 y 4.1, iSCSI, canal de fibra y FCoE.

Independientemente de qué protocolo de almacenamiento se use, los extremos de protocolo proporcionan acceso uniforme al almacenamiento SAN y NAS. Un volumen virtual, como un archivo en otro almacén de datos tradicional, se presenta en una máquina virtual como un disco SCSI.

Nota Un contenedor de almacenamiento está dedicado a SCSI o NAS y no se puede compartir entre esos tipos de protocolo. Una matriz puede presentar un contenedor de almacenamiento con extremos de protocolo SCSI y un contenedor diferente con extremos de protocolo NFS. El contenedor no puede usar una combinación de extremos de protocolo SCSI y NFS.

Transportes basados en Virtual Volumes y SCSI

En las matrices de discos, Virtual Volumes admite protocolos de canal de fibra, FCoE e iSCSI.

Cuando se usa el protocolo basado en SCSI, el extremo de protocolo representa un LUN de proxy definido por un WWN de LUN basado en T10.

Como cualquier LUN basado en bloques, los extremos de protocolo se detectan mediante comandos de detección de LUN estándar. El host ESXi vuelve a examinar periódicamente para encontrar dispositivos nuevos y detecta de manera asíncrona extremos de protocolo basados en bloques. Es posible acceder al extremo de protocolo mediante varias rutas de acceso. El tráfico en esas rutas de acceso sigue directivas de selección de rutas de acceso conocidas, como es común para los LUN.

En matrices de disco basadas en SCSI durante la creación de la máquina virtual, ESXi crea un volumen virtual y lo formatea como VMFS. Este pequeño volumen virtual almacena todos los archivos de metadatos de la máquina virtual y se conoce como config-vVol. config-vVol funciona como un localizador de almacenamiento de máquinas virtuales en vSphere.

Virtual Volumes en las matrices de discos admite el mismo conjunto de comandos SCSI que VMFS, y utiliza ATS como mecanismo de bloqueo.

Compatibilidad con CHAP para endpoints iSCSI

Virtual Volumes admite el protocolo de autenticación por desafío mutuo (Challenge Handshake Access Protocol, CHAP) con destinos iSCSI. Esta compatibilidad permite que los hosts ESXi compartan credenciales de iniciador de CHAP con proveedores de almacenamiento de Virtual Volumes, también denominados proveedores VASA, y que los proveedores de almacenamiento de Virtual Volumes generen eventos del sistema que notifican a vCenter Server los cambios en las credenciales de destino de CHAP en la matriz de almacenamiento.

Cada host ESXi puede tener varios HBA y cada HBA puede tener propiedades configuradas. Una de estas propiedades es el método de autenticación que debe utilizar el HBA. La autenticación es opcional, pero, si se implementa, tanto el iniciador como el destino deben admitirla. CHAP es un método de autenticación que puede usarse en ambas direcciones entre el iniciador y el destino.

Para obtener más información sobre los distintos métodos de autenticación de CHAP, consulte Selección del método de autenticación de CHAP. Para configurar CHAP en su host ESXi, consulte Configurar los parámetros de CHAP para los adaptadores de almacenamiento de iSCSI o iSER.

Transportes de Virtual Volumes y NFS

Con el almacenamiento NAS, un extremo de protocolo es un recurso compartido de NFS que el host ESXi monta mediante la dirección IP o el nombre de DNS y un nombre de recurso compartido. Virtual Volumes admite NFS versión 3 y 4.1 para acceder al almacenamiento NAS. Se admiten los formatos IPv4 e IPv6.

Sin importar la versión que se utilice, una matriz de almacenamiento puede proporcionar varios extremos de protocolo para fines de disponibilidad.

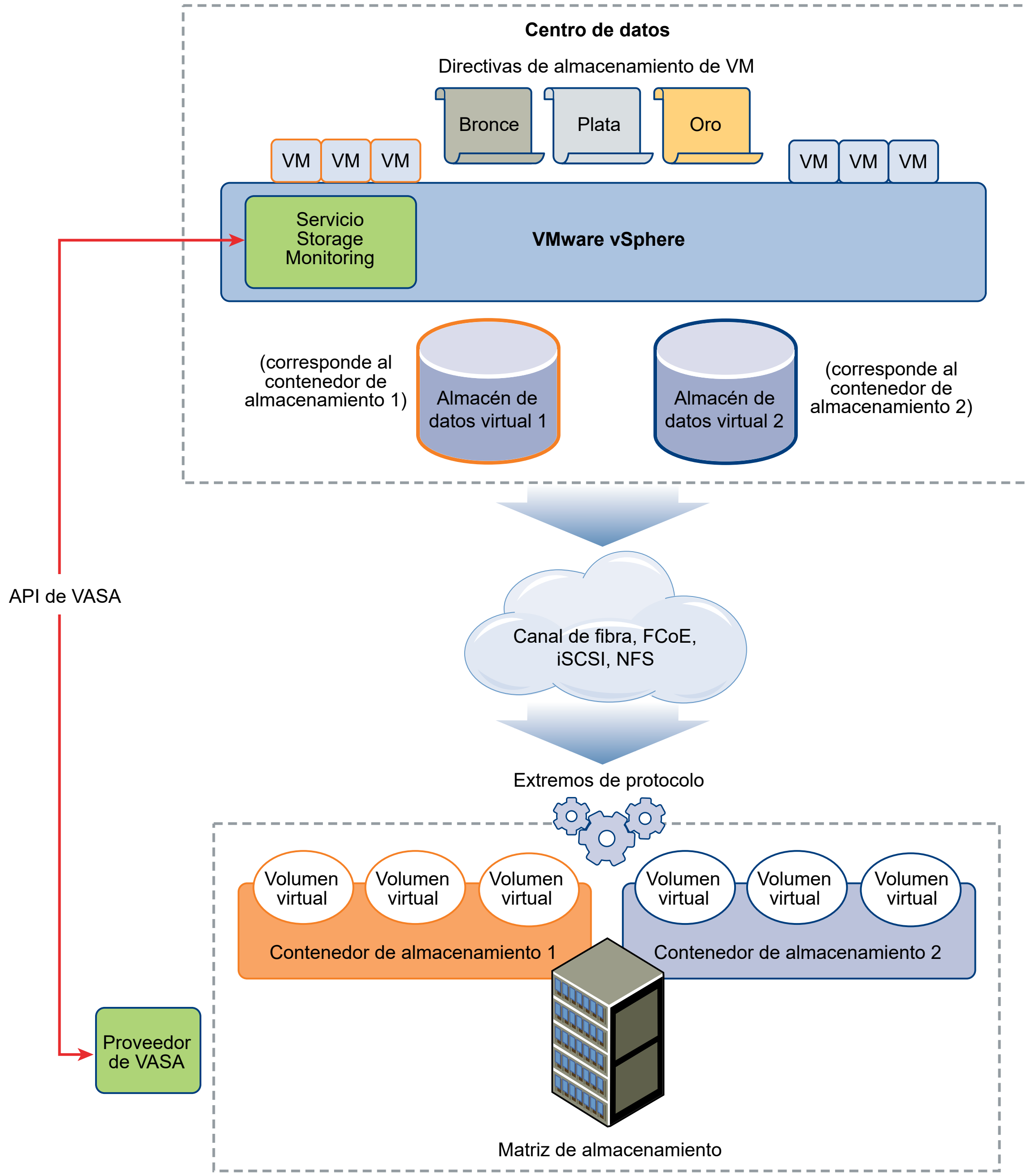
Además, la versión 4.1 de NFS presenta mecanismos de enlace troncal que habilitan el equilibrio de carga y múltiples rutas.

Virtual Volumes en los dispositivos NAS admite las mismas llamadas a procedimiento remoto (Remote Procedure Calls, RPC) de NFS que los hosts ESXi usan al conectarse a puntos de montaje de NFS.

En los dispositivos NAS, config-vVol es un subárbol de directorio que corresponde a un config-vVolID. config-vVol debe admitir directorios y otras operaciones necesarias para NFS.

Arquitectura de Virtual Volumes

Un diagrama arquitectónico proporciona una descripción general de cómo todos los componentes de la funcionalidad de Virtual Volumes interactúan entre sí.



Los volúmenes virtuales son objetos exportados por un sistema de almacenamiento conforme y generalmente se corresponden uno a uno con un disco de máquina virtual y otros archivos relacionados con la máquina virtual. Un proveedor VASA crea y manipula un volumen virtual fuera de banda, no en la ruta de acceso a los datos.

Un proveedor VASA, o un proveedor de almacenamiento, se desarrolla a través de vSphere API for Storage Awareness. El proveedor de almacenamiento habilita la comunicación entre los hosts ESXi, vCenter Server y vSphere Client por una parte, y el sistema de almacenamiento, por otra. El proveedor VASA se ejecuta del lado del almacenamiento y se integra con el servicio de

supervisión de almacenamiento (vSphere Storage Monitoring, SMS) de vSphere para administrar todos los aspectos del almacenamiento de Virtual Volumes. El proveedor VASA asigna objetos de disco virtual y sus derivados, como clones, instantáneas y réplicas, directamente a los volúmenes virtuales del sistema de almacenamiento.

Los hosts ESXi no tienen acceso directo al almacenamiento de volúmenes virtuales. En su lugar, los hosts acceden a los volúmenes virtuales a través de un punto intermedio en la ruta de acceso de datos, denominado extremo de protocolo. Los extremos de protocolo establecen una ruta de acceso de datos a petición desde las máquinas virtuales hacia sus volúmenes virtuales respectivos. Los extremos de protocolo sirven como puerta de enlace para E/S dentro de banda directas entre los hosts ESXi y el sistema de almacenamiento. ESXi puede utilizar los protocolos de Fibre Channel, FCoE, iSCSI y NFS para la comunicación dentro de banda.

Los volúmenes virtuales residen dentro de los contenedores de almacenamiento que lógicamente representan un grupo de discos físicos en el sistema de almacenamiento. En el lado de vCenter Server y ESXi, los contenedores de almacenamiento se presentan como almacenes de datos de Virtual Volumes. Un solo contenedor de almacenamiento puede exportar varios conjuntos de capacidad de almacenamiento y proporcionar diferentes niveles de servicio a diferentes volúmenes virtuales.

Mire el video para obtener información sobre la arquitectura de Virtual Volumes.

(Virtual Volumes Parte 2: Arquitectura)

Virtual Volumes y la entidad de certificación de VMware

vSphere incluye VMware Certificate Authority (VMCA). De manera predeterminada, VMCA crea todos los certificados internos que se utilizan en el entorno de vSphere. Genera certificados para los hosts ESXi recientemente agregados y los proveedores VASA de almacenamiento que administran o representan sistemas de almacenamiento de Virtual Volumes.

Los certificados SSL protegen la comunicación con el proveedor VASA. Estos certificados provienen del proveedor VASA o de VMCA.

- Estos certificados pueden provenir directamente del proveedor VASA para el uso a largo plazo. Pueden ser autogenerados y autofirmados, o bien derivar de una entidad de certificación externa.
- VMCA puede generar los certificados para que el proveedor VASA los utilice.

Cuando se registran un host o un proveedor VASA, VMCA sigue estos pasos automáticamente, sin avisarle al administrador de vSphere.

1 Cuando se agrega un proveedor VASA por primera vez al servicio de administración de almacenamiento (Storage Management Service, SMS) de vCenter Server, se genera un certificado autofirmado.

2 Después de comprobar el certificado, SMS pide una solicitud de firma del certificado (Certificate Signing Request, CSR) del proveedor VASA.

3 Después de recibir y validar la CSR, SMS la presenta a VMCA en nombre del proveedor VASA y solicita un certificado firmado por una entidad de certificación.

   Es posible configurar VMCA para que funcione como entidad de certificación independiente o como subordinada a una entidad de certificación empresarial. Si se configura VMCA como una entidad de certificación subordinada, VMCA firma la CSR con la cadena completa.

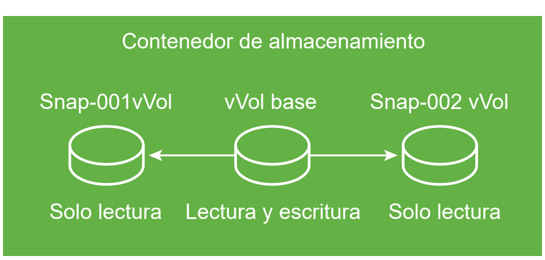
4 El certificado firmado con el certificado raíz se envía al proveedor VASA. El proveedor VASA puede autenticar todas la conexiones seguras futuras provenientes de SMS en vCenter Server y en los hostsESXi.

Instantáneas de Virtual Volumes

Las snapshots conservan el estado y los datos de una máquina virtual en el momento que crea dicha snapshot. Las snapshots son útiles cuando es necesario volver en repetidas ocasiones al mismo estado de la máquina virtual, pero no se desea crear varias máquinas virtuales. Las snapshots de Virtual Volumes cumplen muchas funciones. Puede utilizarlos para crear una copia en modo inactivo para fines de copia de seguridad o de archivo, o bien para crear un entorno de prueba y reversión para aplicaciones. También puede utilizarlos para aprovisionar imágenes de aplicación de forma instantánea.

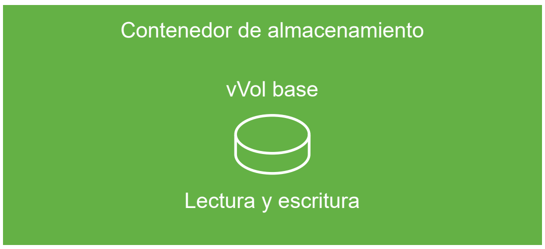
En el entorno de Virtual Volumes, ESXi y vCenter Server son los encargados de la administración de instantáneas, pero estas se ejecutan en la matriz de almacenamiento.

Cada instantánea crea un objeto de volumen virtual adicional, un volumen virtual de instantánea, que tiene el contenido de la memoria de la máquina virtual. Los datos originales de la máquina virtual se copian en este objeto y se conservan en formato de solo lectura, lo cual impide que el sistema operativo invitado escriba en la snapshot. No es posible cambiar el tamaño del volumen virtual de la snapshot. En general, cuando se replica la máquina virtual, también se replica su volumen virtual de snapshot.



El volumen virtual de base permanece activo o en formato de lectura-escritura. Cuando se crea otra snapshot, esta conserva el nuevo estado y los datos de una máquina virtual en el momento que se crea dicha snapshot.

Cuando se eliminan instantáneas, solo se mantiene el volumen virtual de base, mientras que los objetos del volumen virtual de instantáneas se descartan. El volumen virtual de base representa el estado más actual de la máquina virtual. A diferencia de las instantáneas presentes en los almacenes de datos tradicionales, los volúmenes virtuales de instantáneas no necesitan confirmar su contenido en el volumen virtual de base.



Para obtener información sobre la creación y la administración de snapshots, consulte la documentación de *Administrar máquinas virtuales de vSphere*.

Antes de habilitar Virtual Volumes

Para trabajar con Virtual Volumes, debe asegurarse de que el almacenamiento y el entorno de vSphere estén configurados correctamente.

Preparar el sistema de almacenamiento para Virtual Volumes

Para preparar el entorno del sistema de almacenamiento para Virtual Volumes, siga estas instrucciones. Para obtener información adicional, póngase en contacto con el proveedor de almacenamiento.

- El sistema de almacenamiento o la matriz de almacenamiento que utiliza deben admitir Virtual Volumes e integrarse con los componentes de vSphere a través de vSphere API for Storage Awareness (VASA). La matriz de almacenamiento debe admitir el aprovisionamiento fino y la captura de snapshots.
- Se debe implementar el proveedor de almacenamiento de Virtual Volumes.
- Deben configurarse los siguientes componentes en el lado de almacenamiento:
  - Extremos de protocolo
  - Contenedores de almacenamiento
  - Perfiles de almacenamiento
  - Configuraciones de replicación, si piensa utilizar Virtual Volumes con replicación. Consulte Requisitos para la replicación con Virtual Volumes.

Preparar el entorno de vSphere

- Asegúrese de seguir las instrucciones de instalación específicas del tipo de almacenamiento que utilice, Fibre Channel, FCoE, iSCSI o NFS. Si es necesario, instale y configure los adaptadores de almacenamiento en los hosts ESXi.
  - Si utiliza iSCSI, active los adaptadores de iSCSI en los hosts ESXi. Configure la detección dinámica y escriba la dirección IP del sistema de almacenamiento de Virtual Volumes. Consulte Configurar adaptador de iSCSI de software.
- Sincronice todos los componentes en la matriz de almacenamiento con vCenter Server y todos los hosts ESXi. Utilice el protocolo Network Time Protocol (NTP) para realizar esta sincronización.

Para obtener más información, comuníquese con su proveedor y consulte *Guía de compatibilidad de VMware*

Sincronizar el entorno de almacenamiento de vSphere con un servidor horario de red

Si usa Virtual Volumes, configure el protocolo de tiempo de red (Network Time Protocol , NTP) para asegurarse de que todos los hosts ESXi en la red de vSphere estén sincronizados.

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Sistema**, seleccione **Configuración de hora**.
4. Haga clic en **Editar** y configure el servidor NTP.
   a. Seleccione **Usar protocolo de hora de red (Habilitar el cliente NTP)**.
   b. Establezca la directiva de inicio del servicio NTP.
   c. Introduzca la dirección IP del servidor NTP con el que desea realizar la sincronización.
   d. En la sección Estado del servicio NTP, haga clic en **Iniciar** o **Reiniciar**.
5. Haga clic en **Aceptar**.

   El host se sincroniza con el servidor NTP.

Configuración de Virtual Volumes

Para configurar el entorno de Virtual Volumes, debe seguir diversos pasos.

Requisitos previos

Siga las instrucciones que se incluyen en Antes de habilitar Virtual Volumes.

Procedimiento

1 Registrar proveedores de almacenamiento de Virtual Volumes

   El entorno de Virtual Volumes debe incluir proveedores de almacenamiento, también llamados proveedores VASA. Por lo general, los distribuidores independientes desarrollan proveedores de almacenamiento a través de VMware API for Storage Awareness (VASA). Los proveedores de almacenamiento facilitan la comunicación entre vSphere y el lado de almacenamiento. Use vSphere Client para registrar los proveedores de almacenamiento de Virtual Volumes.

2 Crear un almacén de datos de Virtual Volumes

   Puede utilizar el asistente **Nuevo almacén de datos** para crear un almacén de datos de Virtual Volumes.

3 Revisar y administrar extremos de protocolo

   Los hosts ESXi utilizan un proxy de E/S lógico, denominado extremo de protocolo, para comunicarse con volúmenes virtuales y archivos de discos virtuales que los volúmenes virtuales encapsulan. A través de un proveedor de almacenamiento, el sistema de almacenamiento exporta los extremos de protocolo junto con los contenedores de almacenamiento asociados. Los puntos de acceso de protocolo se vuelven visibles en vSphere Client después de asignar un contenedor de almacenamiento a un almacén de datos de Virtual Volumes. Es posible revisar las propiedades de los extremos de protocolo y modificar opciones especiales.

4 (opcional) Cambiar la directiva de selección de rutas de acceso para un extremo de protocolo

   Si el host ESXi utiliza transporte basado en SCSI para comunicarse con extremos de protocolo que representan a una matriz de almacenamiento, se pueden modificar las directivas de múltiples rutas asignadas a los extremos de protocolo. Utilice el cuadro de diálogo **Editar directivas de múltiples rutas** para cambiar una directiva de selección de rutas de acceso.

Pasos siguientes

Ahora puede aprovisionar máquinas virtuales en el almacén de datos de Virtual Volumes. Para obtener información sobre cómo crear máquinas virtuales, consulte la documentación de *Administrar máquinas virtuales de vSphere* y Aprovisionar máquinas virtuales en almacenes de datos de Virtual Volumes.

Registrar proveedores de almacenamiento de Virtual Volumes

El entorno de Virtual Volumes debe incluir proveedores de almacenamiento, también llamados proveedores VASA. Por lo general, los distribuidores independientes desarrollan proveedores de almacenamiento a través de VMware API for Storage Awareness (VASA). Los proveedores de almacenamiento facilitan la comunicación entre vSphere y el lado de almacenamiento. Use vSphere Client para registrar los proveedores de almacenamiento de Virtual Volumes.

Después de realizar el registro, el proveedor de Virtual Volumes se comunica con vCenter Server. El proveedor informa acerca de las características del almacenamiento subyacente y los servicios de datos proporcionados por el sistema de almacenamiento, como la replicación. Las características aparecen en la interfaz de las directivas de almacenamiento de máquina virtual y pueden usarse para crear una directiva de almacenamiento de máquina virtual compatible con el almacén de datos de Virtual Volumes. Después de aplicar esta directiva de almacenamiento a una máquina virtual, la directiva se aplica al almacenamiento de Virtual Volumes. Esta directiva aplica una selección óptima de la máquina virtual dentro del almacenamiento de Virtual Volumes y garantiza que el almacenamiento pueda satisfacer los requisitos de la máquina virtual. Si el almacenamiento proporciona servicios adicionales, como el almacenamiento en caché o la replicación, la directiva habilita estos servicios para la máquina virtual.

Requisitos previos

Verifique que se haya instalado una versión apropiada del proveedor de almacenamiento de Virtual Volumes en el lado de almacenamiento. Obtenga las credenciales del proveedor de almacenamiento.

Procedimiento

1 Desplácese hasta vCenter Server.
2 Haga clic en la pestaña **Configurar** y, a continuación, en **Proveedores de almacenamiento**.
3 Haga clic en el icono **Agregar**.
4 Introduzca la información de conexión del proveedor de almacenamiento, incluidos el nombre, la URL y las credenciales.
5 Especifique el método de seguridad.

Acción	Descripción
Dirigir vCenter Server al certificado del proveedor de almacenamiento	Seleccione la opción **Usar certificado de proveedor de almacenamiento** y especifique la ubicación del certificado.
Utilizar una huella digital del certificado del proveedor de almacenamiento	Si no guía a vCenter Server hasta el certificado del proveedor, se muestra la huella digital del certificado. Revise la huella digital y apruébela. vCenter Server agrega el certificado al almacén de confianza y procede con la conexión.

El proveedor de almacenamiento agrega el certificado de vCenter Server al almacén de confianza cuando vCenter Server se conecta por primera vez al proveedor.

6 Para completar el proceso de registro, haga clic en **Aceptar**.

Resultados

vCenter Server detecta y registra el proveedor de almacenamiento de Virtual Volumes.

Crear un almacén de datos de Virtual Volumes

Puede utilizar el asistente **Nuevo almacén de datos** para crear un almacén de datos de Virtual Volumes.

Procedimiento

1 En el navegador de objetos de vSphere Client, vaya hasta un host, un clúster o un centro de datos.

2 En el menú contextual, seleccione **Almacenamiento > Nuevo almacén de datos**.

3 Seleccione **vVol** como tipo de almacén de datos.

4 Introduzca el nombre del almacén de datos y seleccione un contenedor de almacenamiento de respaldo en la lista de contenedores de almacenamiento.

   Asegúrese de utilizar un nombre que no duplique el de otro almacén de datos en el entorno del centro de datos.

   Si monta el mismo almacén de datos de Virtual Volumes en varios hosts, el nombre del almacén de datos debe ser uniforme entre todos los hosts.

5 Seleccione los hosts que requieren acceso al almacén de datos.

6 Revise las opciones de configuración y haga clic en **Finalizar**.

Pasos siguientes

Después de crear el almacén de datos de Virtual Volumes, puede realizar operaciones de almacenes de datos, como cambiar el nombre del almacén de datos, explorar los archivos del almacén de datos, desmontar el almacén de datos, etc.

No puede agregar el almacén de datos de Virtual Volumes a un clúster de almacenes de datos.

Revisar y administrar extremos de protocolo

Los hosts ESXi utilizan un proxy de E/S lógico, denominado extremo de protocolo, para comunicarse con volúmenes virtuales y archivos de discos virtuales que los volúmenes virtuales encapsulan. A través de un proveedor de almacenamiento, el sistema de almacenamiento exporta los extremos de protocolo junto con los contenedores de almacenamiento asociados. Los puntos de acceso de protocolo se vuelven visibles en vSphere Client después de asignar un contenedor de almacenamiento a un almacén de datos de Virtual Volumes. Es posible revisar las propiedades de los extremos de protocolo y modificar opciones especiales.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Endpoints de protocolo**.

4 Para ver los detalles de un elemento específico, selecciónelo en la lista.

5 Utilice las pestañas en Detalles del extremo de protocolo para acceder a información adicional y modificar las propiedades del extremo de protocolo seleccionado.

Tabulador	Descripción
Propiedades	Muestra las propiedades y las características del elemento. Para los elementos SCSI (en bloque), muestra directivas de múltiples rutas y permite editarlas.
Rutas de acceso (solo extremos de protocolo SCSI)	Muestra las rutas de acceso disponibles para el extremo de protocolo. Permite deshabilitar o habilitar una ruta de acceso seleccionada. Permite cambiar la directiva de selección de rutas de acceso.
Almacenes de datos	Muestre el almacén de datos de Virtual Volumes correspondiente. Permite realizar operaciones de administración de almacenes de datos.

Cambiar la directiva de selección de rutas de acceso para un extremo de protocolo

Si el host ESXi utiliza transporte basado en SCSI para comunicarse con extremos de protocolo que representan a una matriz de almacenamiento, se pueden modificar las directivas de múltiples rutas asignadas a los extremos de protocolo. Utilice el cuadro de diálogo **Editar directivas de múltiples rutas** para cambiar una directiva de selección de rutas de acceso.

Procedimiento

1 En vSphere Client, desplácese hasta el host ESXi.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Endpoints de protocolo**.

4 Seleccione el extremo de protocolo cuyas rutas de acceso desea cambiar y haga clic en la pestaña **Propiedades**.

5 En Directivas de múltiples rutas, seleccione **Editar múltiples rutas** en el menú **Acciones**.

6 Seleccione una directiva de ruta de acceso y configure sus opciones. Las opciones cambian según el tipo de dispositivo de almacenamiento que se utilice.

   Las directivas de ruta de acceso disponibles para la selección dependen de la compatibilidad del proveedor de almacenamiento.

   - Para obtener información sobre las directivas de ruta de acceso para dispositivos SCSI, consulte Directivas y complementos de selección de rutas de acceso.
   - Para obtener información sobre los mecanismos de ruta de acceso para dispositivos NVMe, consulte Complemento de alto rendimiento de VMware y esquemas de selección de rutas de acceso.

7 Para guardar la configuración y salir del cuadro de diálogo, haga clic en **Aceptar**.

Aprovisionar máquinas virtuales en almacenes de datos de Virtual Volumes

Puede aprovisionar máquinas virtuales en un almacén de datos de Virtual Volumes.

Nota Todos los discos virtuales que aprovisione en un almacén de datos de Virtual Volumes deben ser un múltiplo par de 1 MB.

Una máquina virtual que se ejecute en un almacén de datos de Virtual Volumes necesita una directiva de almacenamiento de máquina virtual apropiada.

Después de aprovisionar la máquina virtual, es posible realizar las tareas de administración de máquina virtual típicas. Para obtener información, consulte el documento *Administrar máquinas virtuales de vSphere*.

Procedimiento

1 Defina una directiva de almacenamiento de máquina virtual para Virtual Volumes.

   VMware proporciona una directiva de almacenamiento predeterminada de sin requisitos para Virtual Volumes. Si es necesario, puede crear una directiva de almacenamiento personalizada que sea compatible con Virtual Volumes.

   Consulte Crear una directiva de almacenamiento de máquina virtual para Virtual Volumes.

2 Asigne la directiva de almacenamiento de máquina virtual de Virtual Volumes a la máquina virtual.

   Para garantizar que el almacén de datos de Virtual Volumes cumpla con los requisitos de almacenamiento específicos cuando asigne una máquina virtual, asocie la directiva de almacenamiento de Virtual Volumes con la máquina virtual.

   Consulte Asignar directivas de almacenamiento a máquinas virtuales.

3 Cambie la directiva de almacenamiento predeterminada de un almacén de datos de Virtual Volumes.

   Para máquinas virtuales aprovisionadas en almacenes de datos de Virtual Volumes, VMware ofrece una directiva de sin requisitos predeterminada. No es posible editar esta directiva, pero se puede designar una directiva recién creada como la predeterminada.

   Consulte Cambiar la directiva de almacenamiento predeterminada de un almacén de datos.

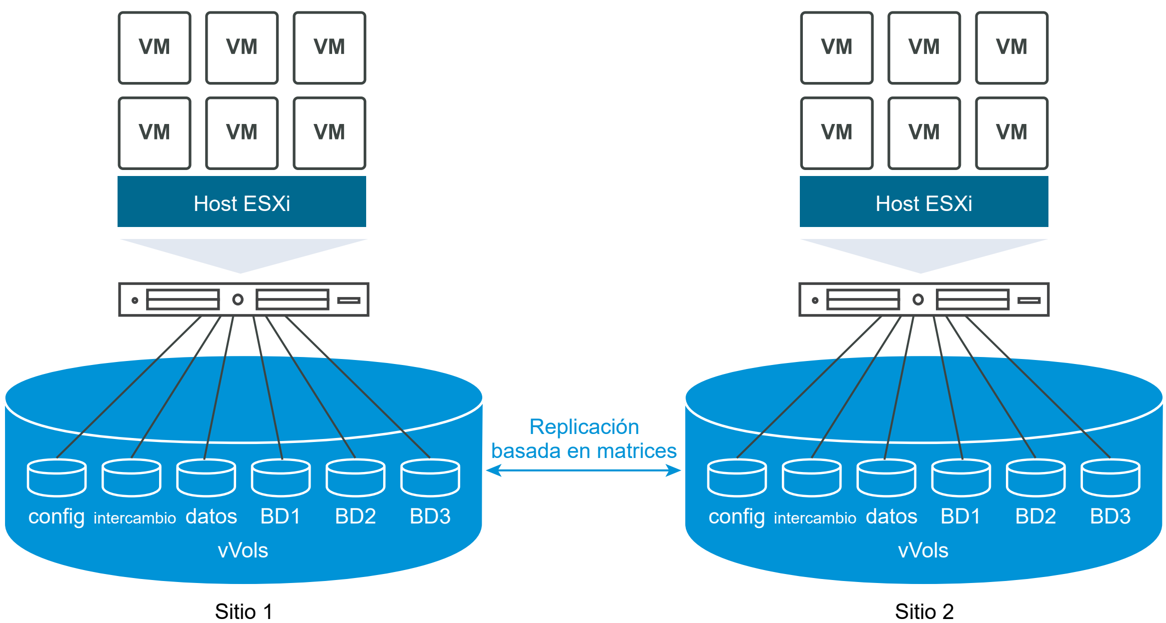
Virtual Volumes y la replicación

Virtual Volumes admite la replicación y la recuperación ante desastres. La replicación basada en matrices permite descargar la replicación de máquinas virtuales en la matriz de almacenamiento y usar las capacidades de replicación completas de la matriz. Puede replicar un solo objeto de máquina virtual, como un disco virtual. También puede agrupar varios objetos de máquina virtual o varias máquinas virtuales para replicarlos como una sola unidad.

La replicación basada en matrices está controlada por directivas. Después de configurar el almacenamiento de Virtual Volumes para la replicación, el proveedor de almacenamiento proporciona, a partir de la matriz, información acerca de las capacidades de replicación y los grupos de replicación. Esta información se muestra en la interfaz de la directiva de almacenamiento de la máquina virtual de vCenter Server.

Utilice la directiva de almacenamiento de máquina virtual para describir los requisitos de replicación para las máquinas virtuales. Los parámetros que especifica en la directiva de almacenamiento dependen de cómo la matriz implementa la replicación. Por ejemplo, la directiva de almacenamiento de máquina virtual puede incluir parámetros como la programación de replicación, la frecuencia de replicación o el objetivo de punto de recuperación (Recovery Point Objective, RPO). La directiva también puede indicar el destino de replicación, un sitio secundario donde se replican las máquinas virtuales, o especificar si se deben eliminar las réplicas.

Al asignar la directiva de replicación durante el aprovisionamiento de la máquina virtual, debe solicitar servicios de replicación para la máquina virtual. Posteriormente, la matriz se encarga de la administración de todas las programaciones y los procesos de replicación.



Requisitos para la replicación con Virtual Volumes

Cuando se habilita Virtual Volumes con replicación, además de los requisitos generales de Virtual Volumes, el entorno debe cumplir con varios requisitos previos específicos.

Para conocer los requisitos generales de Virtual Volumes, consulte Antes de habilitar Virtual Volumes.

Requisitos de almacenamiento

La implementación de la replicación de Virtual Volumes depende de la matriz y puede diferir para otros proveedores de almacenamiento. En general, se aplican los siguientes requisitos a todos los proveedores.

- Las matrices de almacenamiento que se usen para implementar la replicación deben ser compatibles con Virtual Volumes.
- Las matrices deben integrarse a la versión del proveedor de almacenamiento (VMware API for Storage Awareness, VASA) compatible con la replicación de Virtual Volumes.
- Las matrices de almacenamiento deben tener capacidad de replicación y deben estar configuradas para poder usar mecanismos de replicación proporcionados por el proveedor. Las configuraciones típicas generalmente implican uno o dos destinos de replicación. Toda configuración requerida, como el emparejamiento del sitio replicado y del sitio de destino, también debe implementarse en el lado del almacenamiento.
- Cuando corresponda, los grupos de replicación y los dominios de errores de Virtual Volumes deben estar previamente configurados en el lado del almacenamiento.

Para obtener más información, comuníquese con su proveedor y consulte *Guía de compatibilidad de VMware*.

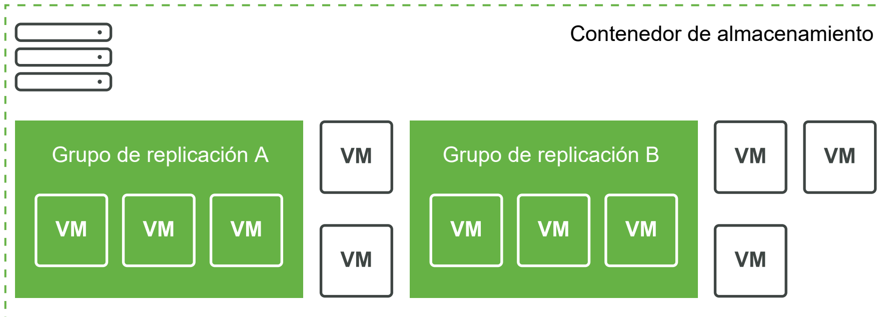
Requisitos de vSphere

- Utilice las versiones de vCenter Server y de ESXi que admitan la replicación de almacenamiento de Virtual Volumes. vCenter Server y los hosts ESXi de versiones anteriores a 6.5 no admiten el almacenamiento replicado de Virtual Volumes. Cualquier intento de crear una máquina virtual replicada en un host incompatible generará un error. Para obtener información, consulte *Guía de compatibilidad de VMware*.
- Si desea migrar una máquina virtual, asegúrese de que los recursos de destino, como los hosts ESXi y los almacenes de datos de Virtual Volumes, admitan la replicación de almacenamiento.

Virtual Volumes y grupos de replicación

Cuando un almacenamiento ofrece servicios de replicación, además de contenedores de almacenamiento y extremos de protocolo, el administrador de almacenamiento puede configurar grupos de replicación en el lado del almacenamiento.

vCenter Server y ESXi pueden detectar grupos de replicación, pero no administrar su ciclo de vida. Los grupos de replicación, también conocidos como grupos de consistencia, indican qué máquinas virtuales y discos virtuales deben replicarse juntos en un sitio de destino. Es posible asignar componentes de una misma máquina virtual, como el archivo de configuración de máquina virtual y discos virtuales, a diferentes grupos de replicación preconfigurados. O bien, es posible excluir de la replicación ciertos componentes de la máquina virtual.



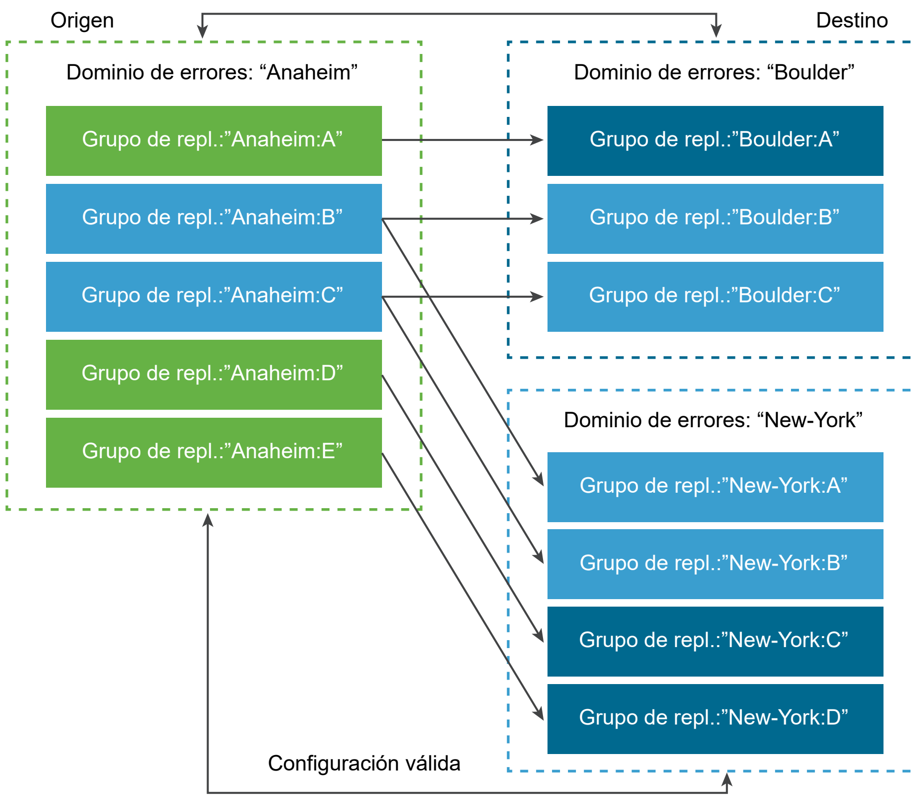
Si no existen grupos preconfigurados disponibles, Virtual Volumes puede usar un método automático. Con el método automático, Virtual Volumes crea un grupo de replicación a pedido y asocia ese grupo a un objeto de Virtual Volumes que se esté aprovisionando. Si se utiliza el grupo de replicación automático, se asignan todos los componentes de una máquina virtual al grupo. No se pueden mezclar grupos de replicación preconfigurados y automáticos para los componentes de una misma máquina virtual.

Virtual Volumes y dominios de errores

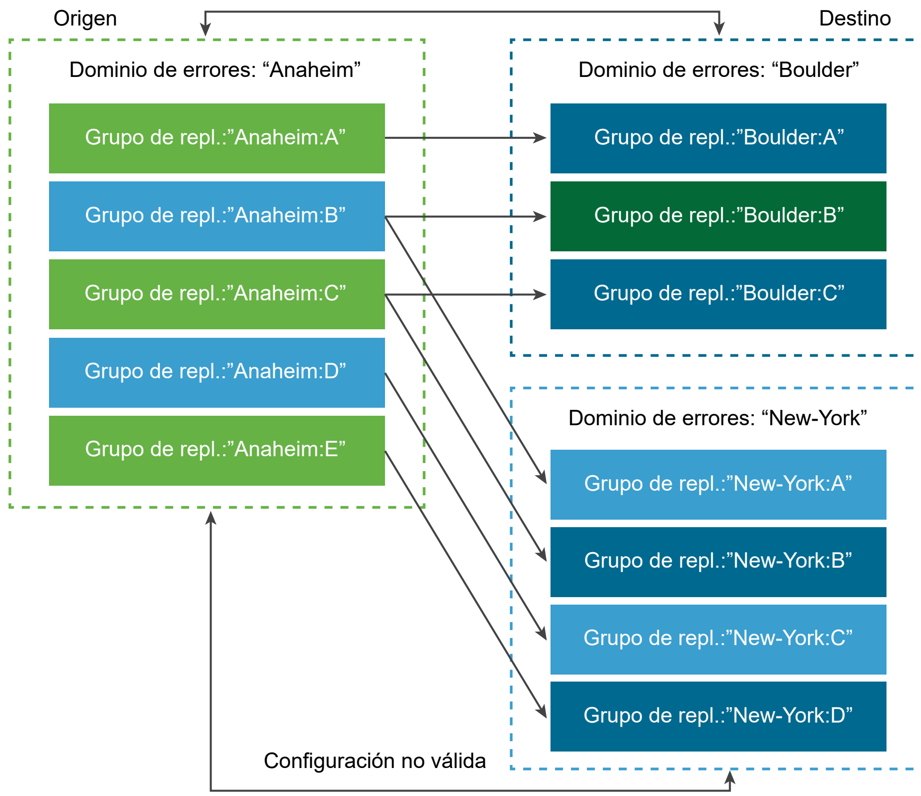
En el entorno de Virtual Volumes, los dominios de errores definen cómo deben combinarse los grupos de replicación específicos al replicarse de un sitio de origen a un sitio de destino.

Los dominios de errores se configuran e informan mediante la matriz de almacenamiento, pero no se exponen en vSphere Client. El mecanismo de administración de almacenamiento basada en directivas (Storage Policy Based Management, SPBM) detecta los dominios de errores y los usa para realizar validaciones durante la creación una máquina virtual.

Por ejemplo, aprovisione una máquina virtual con dos discos: uno asociado con el grupo de replicación Anaheim:B, el otro asociado con el grupo de replicación Anaheim:C. SPBM valida el aprovisionamiento porque ambos discos se replican en los mismos dominios de errores de destino.



Ahora aprovisione una máquina virtual con dos discos, uno asociado con el grupo de replicación Anaheim:B, otro asociado con el grupo de replicación Anaheim:D. Esta configuración no es válida. Ambos grupos de replicación se replican en el dominio de errores New-York. Sin embargo, solo uno se replica en el dominio de errores Boulder.



Flujo de trabajo de replicación de Virtual Volumes

Si en vCenter Server se muestra información sobre las capacidades de replicación de la matriz de almacenamiento de Virtual Volumes, es posible activar la replicación de las máquinas virtuales.

El flujo de trabajo para activar la replicación de las máquinas virtuales incluye pasos típicos del aprovisionamiento de máquinas virtuales en el almacenamiento de Virtual Volumes.

1 Defina una directiva de almacenamiento de máquina virtual que sea compatible con el almacenamiento de replicación. Las reglas basadas en el almacén de datos de la directiva deben incluir el componente de replicación. Consulte Crear una directiva de almacenamiento de máquina virtual para Virtual Volumes.

   Una vez configurada la directiva de almacenamiento que incluye la replicación, vCenter Server detecta los grupos de replicación disponibles.

2 Asigne la directiva de replicación a la máquina virtual. Si está configurado, seleccione un grupo de replicación compatible, o use la asignación automática. Consulte Asignar directivas de almacenamiento a máquinas virtuales.

Directrices y consideraciones de la replicación

Cuando use replicación con Virtual Volumes, corresponden consideraciones específicas.

- Es posible aplicar la directiva de almacenamiento de replicación únicamente a un volumen virtual de configuración y a un volumen virtual de datos. Otros objetos de máquina virtual heredan la directiva de replicación de la siguiente manera:
  - El volumen virtual de memoria hereda la directiva del volumen virtual de configuración.
  - El volumen virtual de resumen hereda la directiva del volumen virtual de datos.
  - El volumen virtual de intercambio, que existe mientras hay una máquina virtual encendida, queda excluido de la replicación.
- Si no se aplica la directiva de replicación al disco de una máquina virtual, el disco no se replica.
- La directiva de almacenamiento de replicación no debe usarse como directiva de almacenamiento predeterminada para un almacén de datos. De lo contrario, la directiva no permite que se seleccionen grupos de replicación.
- La replicación conserva el historial de snapshots. Si se creó y se replicó una snapshot, es posible recuperar la snapshot coherente de las aplicaciones.
- Es posible replicar un clon vinculado. Si se replica un clon vinculado sin su elemento principal, se convierte en un clon completo.
- Si un archivo de descriptor pertenece a un disco virtual de una máquina virtual, pero reside en el inicio de otra máquina virtual, ambas máquinas virtuales deben encontrarse en el mismo grupo de replicación. Si las máquinas virtuales se encuentran en diferentes grupos de replicación, los dos grupos deben conmutarse por error al mismo tiempo. De lo contrario, el descriptor podría dejar de estar disponible después de la conmutación por error. Como consecuencia, la máquina virtual podría no encenderse.
- En Virtual Volumes con entorno de replicación, podrá ejecutar un flujo de trabajo de conmutación por error de prueba de forma periódica para asegurarse de que las cargas de trabajo recuperadas funcionan tras una conmutación por error.

  Las máquinas virtuales de prueba que se creen durante la conmutación por error de prueba son completamente funcionales y adecuadas para operaciones administrativas generales. No obstante, se deben tener en cuenta ciertos aspectos:
  - Las máquinas virtuales creadas durante una conmutación por error de prueba se deben eliminar antes de que la conmutación por error de prueba se detenga. La eliminación garantiza que las instantáneas o los volúmenes virtuales relacionados con instantáneas que formen parte de la máquina virtual, como el volumen virtual de instantáneas, no interfieran con la detención de la conmutación por error.
  - Puede crear clones completos de las máquinas virtuales de prueba.

- Solo se pueden crear clones rápidos si la directiva aplicada a la nueva máquina virtual contiene el mismo identificador de grupo de replicación que la máquina virtual que se clonará. Al intentar colocar la máquina virtual secundaria fuera del grupo de replicación de la máquina virtual principal, se producirá un error.

Prácticas recomendadas para trabajar con Virtual Volumes

Tenga en cuenta estas recomendaciones cuando use Virtual Volumes con ESXi y vCenter Server.

- Directrices y limitaciones al utilizar Virtual Volumes

  Para aprovechar al máximo la funcionalidad de Virtual Volumes, debe seguir unas directrices concretas.

- Prácticas recomendadas para el aprovisionamiento de contenedores de almacenamiento

  Siga estas recomendaciones cuando aprovisione contenedores de almacenamiento en las matrices de Virtual Volumes.

- Prácticas recomendadas para rendimiento de Virtual Volumes

  Para garantizar resultados de rendimiento óptimos de Virtual Volumes, siga estas recomendaciones.

Directrices y limitaciones al utilizar Virtual Volumes

Para aprovechar al máximo la funcionalidad de Virtual Volumes, debe seguir unas directrices concretas.

Virtual Volumes admite las siguientes capacidades, características y productos de VMware:

- Con Virtual Volumes, puede usar servicios avanzados de almacenamiento que incluyen la replicación, el cifrado, la desduplicación y la compresión en discos virtuales individuales. Póngase en contacto con su proveedor de almacenamiento para obtener información sobre los servicios compatibles con Virtual Volumes.
- La funcionalidad de Virtual Volumes admite software de copia de seguridad que usa vSphere API - Data Protection. Los volúmenes virtuales están modelados como los discos virtuales. Los productos de copia de seguridad que usan vSphere APIs - Data Protection son compatibles con los volúmenes virtuales, ya que se encuentran en archivos VMDK de LUN. vSphere y el software de copia de seguridad reconocen las instantáneas que se crean mediante vSphere API - Data Protection como instantáneas que no son de vVols.

  Nota Virtual Volumes no es compatible con el modo de transporte de SAN. vSphere APIs - Data Protection selecciona un método de transferencia de datos alternativo automáticamente.

  Para obtener más información sobre la integración con vSphere Storage APIs - Data Protection, póngase en contacto con su proveedor de software de copia de seguridad.
- Virtual Volumes admite características de vSphere como vSphere vMotion, Storage vMotion, instantáneas, clones vinculados y DRS.

- Con Virtual Volumes se pueden utilizar productos de agrupación en clúster, como Oracle Real Application Clusters. Para utilizar estos productos, active la opción de multiescritura para un disco virtual guardado en el almacén de datos de Virtual Volumes.

Para obtener más detalles, consulte el artículo de la base de conocimientos en http://kb.vmware.com/kb/2112039. Para acceder a un listado de características y productos compatibles con la funcionalidad de Virtual Volumes, consulte las *matrices de interoperabilidad de productos de VMware*.

Limitaciones de Virtual Volumes

Para disfrutar de una experiencia óptima con Virtual Volumes, tenga en cuenta las siguientes limitaciones:

- Debido a que el entorno de Virtual Volumes requiere vCenter Server, Virtual Volumes no se puede utilizar con un host independiente.
- La funcionalidad de Virtual Volumes no es compatible con RDM.
- Un contenedor de almacenamiento de Virtual Volumes no puede abarcar varias matrices físicas. Algunos proveedores presentan varias matrices físicas como una matriz única. En estos casos, técnicamente se sigue utilizando una sola matriz lógica.
- Los perfiles de hosts que contienen almacenes de datos de Virtual Volumes son específicos de vCenter Server. Después de extraer este tipo de perfil de host, solo se puede asociar a los hosts y los clústeres administrados por la misma instancia de vCenter Server que el host de referencia.

Prácticas recomendadas para el aprovisionamiento de contenedores de almacenamiento

Siga estas recomendaciones cuando aprovisione contenedores de almacenamiento en las matrices de Virtual Volumes.

Crear contenedores en función de los límites

Debido a que los contenedores de almacenamiento aplican límites lógicos al agrupar volúmenes virtuales, el contenedor debe coincidir con los límites que desee aplicar.

Algunos ejemplos incluyen un contenedor creado para un arrendatario en una implementación de varios arrendatarios, o un contenedor para un departamento en una implementación empresarial.

- Organizaciones o departamentos, por ejemplo, Recursos humanos o Contabilidad
- Grupos o proyectos, por ejemplo, Equipo A y Equipo rojo
- Clientes

Colocar todas las capacidades de almacenamiento en un solo contenedor

Los contenedores de almacenamiento son almacenes de datos individuales. Un único contenedor de almacenamiento puede exportar varios perfiles de capacidades de almacenamiento. Como resultado, las máquinas virtuales con distintas necesidades y diferente configuración de directivas de almacenamiento pueden ser parte del mismo contenedor de almacenamiento.

El cambio de perfiles de almacenamiento debe realizarse en el lado de las matrices, no como una migración de almacenamiento a otro contenedor.

Evitar el exceso de aprovisionamiento de los contenedores de almacenamiento

Cuando se aprovisiona un contenedor de almacenamiento, los límites de espacio que se aplican durante la configuración del contenedor son solo límites lógicos. No aprovisione el contenedor más de lo necesario para el uso esperado. Si aumenta el tamaño del contenedor más tarde, no tendrá que volver a darle formato ni volver a crear particiones.

Usar la interfaz de usuario de administración específica para el almacenamiento a fin de aprovisionar endpoints de protocolo

Todos los contenedores de almacenamiento necesitan endpoints de protocolo (PE) a los que puedan acceder los hosts ESXi.

Cuando se usa el almacenamiento en bloque, el PE representa un LUN de proxy definido por un WWN de LUN basado en T10. Para el almacenamiento NFS, el PE es un punto de montaje, como una dirección IP o nombre DNS y un nombre del recurso compartido.

Normalmente, la configuración de los PE es específica de la matriz. Al configurar PE, puede que sea necesario asociarlos con procesadores de almacenamiento concretos o con determinados hosts. Para evitar errores al crear PE, no los configure de forma manual. En su lugar, siempre que sea posible, use las herramientas de administración específicas para el almacenamiento.

No asignar identificadores mayores que Disk.MaxLUN a los LUN de los endpoints de protocolo

De forma predeterminada, un host ESXi puede acceder a los identificadores de LUN que estén comprendidos en el intervalo de 0 a 1.023. Si el identificador del LUN del endpoint de protocolo que ha configurado es 1.024 o mayor, el host ignorará el PE.

Si el entorno usa identificadores de LUN mayores que 1023, cambie el número de LUN examinados mediante el parámetro `Disk.MaxLUN`. Consulte Cambiar la cantidad de dispositivos de almacenamiento examinados.

Prácticas recomendadas para rendimiento de Virtual Volumes

Para garantizar resultados de rendimiento óptimos de Virtual Volumes, siga estas recomendaciones.

Usar diferentes directivas de almacenamiento de máquina virtual para componentes de volumen virtual individuales

De forma predeterminada, todos los componentes de una máquina virtual del entorno de Virtual Volumes tienen una sola directiva de almacenamiento de máquina virtual. No obstante, los diferentes componentes pueden tener características de rendimiento diferentes, por ejemplo, un disco virtual de base de datos y su disco virtual de registro correspondiente. En función de los requisitos de rendimiento, puede asignar directivas de almacenamiento de máquina virtual diferentes a discos virtuales individuales y al archivo de inicio de la máquina virtual o a config-vVol.

Cuando se usa vSphere Client, no se puede cambiar la asignación de la directiva de almacenamiento de máquina virtual para swap-vVol, memory-vVol ni snapshot-vVol.

Consulte Crear una directiva de almacenamiento de máquina virtual para Virtual Volumes.

Obtener un perfil de host con Virtual Volumes

La mejor manera de obtener un perfil de host con Virtual Volumes es configurar un host de referencia y, a continuación, extraer su perfil. Si se edita manualmente un perfil de host existente en vSphere Client y luego se asocia el perfil editado a un host nuevo, se pueden producir errores de cumplimiento. Es posible que también se produzcan otros problemas impredecibles. Para obtener más información, consulte el artículo 2146394 de la base de conocimientos de VMware.

Supervisar la carga de E/S en un endpoint de protocolo individual

- Todas las E/S del volumen virtual pasan a través de endpoints de protocolo (PE). Las matrices seleccionan los endpoints de protocolo en los diferentes PE a los que puede acceder un host de ESXi. Las matrices pueden equilibrar la carga y cambiar la ruta de enlace que conecta el volumen virtual con el PE. Consulte Enlazar y desenlazar volúmenes virtuales con extremos de protocolo.
- En el almacenamiento en bloque, ESXi ofrece una gran profundidad de cola a las E/S debido a la posibilidad de que haya muchos volúmenes virtuales. El parámetro `Scsi.ScsiVVolPESNRO` controla la cantidad de E/S que se pueden poner en cola para los PE. Puede configurar el parámetro en la página Configuración avanzada del sistema de vSphere Client.

Supervisar limitaciones de matriz

Una sola máquina virtual puede ocupar varios volúmenes virtuales. Consulte Objetos de Virtual Volumes.

Supongamos que la máquina virtual tiene dos discos virtuales y que se toman dos instantáneas con memoria. La máquina virtual puede ocupar hasta 10 objetos de Virtual Volumes: 1 config-vVol, 1 swap-vVol, 2 data-vVols, 4 snapshot-vVols y 2 snapshot-vVols de memoria.

Garantizar que el proveedor de almacenamiento esté disponible

Para acceder al almacenamiento de Virtual Volumes, el host ESXi requiere un proveedor de almacenamiento (proveedor de VASA). Para asegurar que el proveedor de almacenamiento esté siempre disponible, siga estas directrices:

- No migre ninguna máquina virtual del proveedor de almacenamiento al almacenamiento de Virtual Volumes.
- Realice una copia de seguridad de la máquina virtual del proveedor de almacenamiento.
- Cuando sea necesario, use vSphere HA o Site Recovery Manager para proteger la máquina virtual del proveedor de almacenamiento.

Solucionar problemas en Virtual Volumes

Los temas de solución de problemas ofrecen soluciones para problemas que se podrían encontrar al usar Virtual Volumes.

- Comandos de Virtual Volumes y esxcli

  Puede usar los comandos `esxcli storage vvol` para solucionar problemas en el entorno de Virtual Volumes.

- Recopilar información estadística para Virtual Volumes

  Puede utilizar el comando `vvol stats` en el host de ESXi para realizar un seguimiento de las estadísticas de rendimiento.

- No puede accederse al almacén de datos de Virtual Volumes

  Después de que crea un almacén de datos Virtual Volumes, queda inaccesible.

- Errores durante la migración de máquinas virtuales o durante la implementación de OVF de máquina virtual a almacenes de datos de Virtual Volumes

  Los intentos de migrar una máquina virtual o de implementar una OVF de máquina virtual en almacenes de datos de Virtual Volumes generan errores.

Comandos de Virtual Volumes y esxcli

Puede usar los comandos `esxcli storage vvol` para solucionar problemas en el entorno de Virtual Volumes.

Están disponibles las opciones de comando siguientes.

Tabla 22-1. Comandos `esxcli storage vvol`

Espacio de nombres	Opción de comando	Descripción
`esxcli storage core device`	`list`	Identifique los endpoints de protocolo. La entrada de resultados `Is VVOL PE: true` indica que el dispositivo de almacenamiento es un endpoint de protocolo.
`esxcli storage vvol daemon`	`unbindall`	Desvincula todos los volúmenes virtuales de todos los proveedores de VASA conocidos para el host ESXi.
`esxcli storage vvol protocolendpoint`	`list`	Enumera todos los extremos del protocolo a los que puede tener acceso su host.
`esxcli storage vvol storagecontainer`	`list` `abandonedvvol scan`	Enumere todos los contenedores de almacenamiento disponibles. Explora el contenedor de almacenamiento especificado en busca de volúmenes virtuales abandonados.
`esxcli storage vvol vasacontext`	`get`	Muestre el contexto de VASA (UUID de VC) asociado al host.
`esxcli storage vvol vasaprovider`	`list`	Enumere todos los proveedores (VASA) de almacenamiento asociados al host.

Recopilar información estadística para Virtual Volumes

Puede utilizar el comando `vvol stats` en el host de ESXi para realizar un seguimiento de las estadísticas de rendimiento.

Están disponibles las opciones de comando siguientes.

Comando	Descripción	Opciones
`esxcli storage vvol stats get`	Obtiene estadísticas para todos los proveedores de VASA (valor predeterminado) o para el espacio de nombres o la entidad especificados en el espacio de nombres en cuestión.	`-e|--entity=` *`str`* Introduzca el identificador de entidad. `-n|--namespace=` *`str`* Introduzca la expresión de espacio de nombres del nodo. `-r|--raw` Habilite la salida sin formato.
`esxcli storage vvol stats list`	Enumera todos los nodos estadísticos (valor predeterminado) o los nodos en un espacio de nombres especificado.	`-n|--namespace=` *`str`* Introduzca la expresión de espacio de nombres del nodo.
`esxcli storage vvol stats enable`	Habilita el seguimiento de estadísticas para el espacio de nombres completo.	

Comando	Descripción	Opciones
`esxcli storage vvol stats disable`	Deshabilita el seguimiento de estadísticas para el espacio de nombres completo.	
`esxcli storage vvol stats add`	Habilita el seguimiento de estadísticas para una entidad específica en un espacio de nombres específico.	`-e|--entity=` *str* Introduzca el identificador de entidad. `-n|--namespace=` *str* Introduzca la expresión de espacio de nombres del nodo.
`esxcli storage vvol stats remove`	Elimina una entidad específica para el seguimiento de estadísticas en el espacio de nombres especificado.	`-e|--entity=` *str* Introduzca el identificador de entidad. `-n|--namespace=` *str* Introduzca la expresión de espacio de nombres del nodo.
`esxcli storage vvol stats reset`	Restablece el contador de estadísticas de la entidad o el espacio de nombres de estadísticas especificado.	`-e|--entity=` *str* Introduzca el identificador de entidad. `-n|--namespace=` *str* Introduzca la expresión de espacio de nombres del nodo.

No puede accederse al almacén de datos de Virtual Volumes

Después de que crea un almacén de datos Virtual Volumes, queda inaccesible.

Problema

vSphere Client indica que no es posible acceder al almacén de datos. No se puede usar el almacén de datos para aprovisionamiento de máquinas virtuales.

Causa

Este problema podría ocurrir cuando no configura los extremos del protocolo para el contenedor de almacenamiento basado en SCSI que está asignado al almacén de datos virtual. Al igual que los LUN tradicionales, los extremos del protocolo SCSI deben configurarse de manera que un host ESXi pueda detectarlos.

Solución

Antes de crear almacenes de datos virtuales para contenedores basados en SCSI, asegúrese de configurar extremos del protocolo en el lado de almacenamiento.

Errores durante la migración de máquinas virtuales o durante la implementación de OVF de máquina virtual a almacenes de datos de Virtual Volumes

Los intentos de migrar una máquina virtual o de implementar una OVF de máquina virtual en almacenes de datos de Virtual Volumes generan errores.

Problema

Una plantilla de OVF o una máquina virtual que se migra desde un almacén de datos no virtual pueden incluir archivos adicionales de gran tamaño, como imágenes de disco ISO, imágenes de DVD y archivos de imagen. Si estos archivos adicionales hacen que el volumen virtual de configuración supere su límite de 4 GB, se produce un error en la migración o la implementación en un almacén de datos virtual.

Causa

El volumen virtual de configuración, o config-vVol, contiene diversos archivos relacionados con máquinas virtuales. En los almacenes de datos no virtuales tradicionales, estos archivos se almacenan en el directorio principal de la máquina virtual. De forma similar al directorio principal de la máquina virtual, config-vVol incluye el archivo de configuración de máquina virtual, archivos de disco virtual y descriptor de instantáneas, archivos de registro, archivos de bloqueo, etc.

En los almacenes de datos virtuales, todos los demás archivos de gran tamaño, como discos virtuales, snapshots creadas con memoria, intercambio y resumen, se almacenan en volúmenes virtuales separados.

Los config-vVol se crean como volúmenes virtuales de 4 GB. El contenido genérico de config-vVol generalmente consume solo una fracción de esta asignación de 4 GB, por lo que los config-vVol casi siempre tienen un aprovisionamiento fino para conservar el espacio de copia de seguridad. Todos los archivos adicionales de gran tamaño, como imágenes de disco ISO, imágenes de DVD y archivos de imagen, pueden hacer que config-vVol supere su límite de 4 GB. Si esos archivos se incluyen en una plantilla de OVF, la implementación de OVF de máquina virtual en el almacenamiento de Virtual Volumes genera errores. Si esos archivos son parte de una máquina virtual existente, la migración de esa máquina virtual de un almacén de datos tradicional al almacenamiento de Virtual Volumes también genera errores.

Solución

- Para la migración de máquinas virtuales. Antes de migrar una máquina virtual de un almacén de datos tradicional a un almacén de datos virtual, quite el contenido sobrante del directorio principal de la máquina virtual para que config-vVol no supere el límite de 4 GB.
- Para la implementación de OVF. Ya que no se puede implementar una plantilla de OVF que contenga archivos de más directamente en un almacén de datos virtual, primero se debe implementar la máquina virtual en un almacén de datos no virtual. Quite el contenido de sobra del directorio principal de la máquina virtual y migre esta última al almacenamiento de Virtual Volumes.

Filtrar E/S de máquinas virtuales

23

Los filtros de E/S son componentes de software que pueden instalarse en hosts ESXi y brindar servicios de datos adicionales a las máquinas virtuales. Los filtros procesan solicitudes de E/S, que se desplazan entre el sistema operativo invitado de una máquina virtual y los discos virtuales.

Los filtros de E/S pueden ser suministrados por VMware o creados por terceros mediante vSphere APIs for I/O Filtering (VAIO).

Este capítulo incluye los siguientes temas:

Acerca de los filtros de E/S

Los filtros de E/S pueden obtener acceso directo a la ruta de acceso de E/S de la máquina virtual. Puede habilitar el filtro de E/S para un nivel de disco virtual individual. Los filtros de E/S son independientes de la topología de almacenamiento.

VMware ofrece ciertas categorías de filtros de E/S. Además, otros proveedores pueden crear filtros de E/S. En general, se distribuyen como paquetes que proporcionan un instalador para implementar los componentes de filtro en vCenter Server y en los clústeres de hosts ESXi.

Después de implementar los filtros de E/S, vCenter Server configura y registra un proveedor de almacenamiento de filtro de E/S, también denominado proveedor VASA, para cada host del clúster. Los proveedores de almacenamiento se comunican con vCenter Server y hacen que los servicios de datos ofrecidos por el filtro de E/S estén visibles en la interfaz de directivas de almacenamiento de máquina virtual. Es posible hacer referencia a estos servicios de datos al definir reglas comunes para una directiva de máquina virtual. Después de asociar discos virtuales con esta directiva, los filtros de E/S se habilitan en los discos virtuales.

Compatibilidad con el almacén de datos

Los filtros de E/S pueden admitir todos los tipos de almacenes de datos, incluidos los siguientes:

- VMFS
- NFS 3
- NFS 4.1
- vVol
- vSAN

Tipos de filtros de E/S

VMware proporciona determinadas categorías de filtros de E/S instalados en sus hosts ESXi. Además, los partners de VMware pueden crear los filtros de E/S mediante el programa de desarrolladores vSphere APIs for I/O Filtering (VAIO). Los filtros de E/S pueden servir para diferentes fines.

Los tipos de filtros compatibles incluyen los siguientes:

- Replicación. Replica todas las operaciones de E/S en una ubicación objetivo externa, como otro host o clúster.
- Cifrado. Ofrecido por VMware. Proporciona mecanismos de cifrado para máquinas virtuales. Para obtener más información, consulte la documentación sobre *Seguridad de vSphere*.
- Almacenamiento en caché. Implementa una memoria caché para los datos del disco virtual. El filtro puede usar un dispositivo de almacenamiento flash local para almacenar en caché los datos y aumentar las tasas de utilización de hardware e IOPS para el disco virtual. Si utiliza el filtro de almacenamiento en caché, es posible que deba configurar un recurso flash virtual.
- Storage I/O Control. Ofrecido por VMware. Regula la carga de E/S destinada a un almacén de datos y controla la cantidad de E/S de almacenamiento que se asigna a las máquinas virtuales durante períodos de congestión de E/S. Para obtener más información, consulte la documentación sobre *Administrar recursos de vSphere*.

Nota Puede instalar muchos filtros de la misma categoría, como el almacenamiento en caché, en el host ESXi. No obstante, puede tener un filtro de la misma categoría por disco virtual.

Componentes de los filtros de E/S

En el proceso de filtrado de E/S están involucrados varios componentes.

Algunos de los componentes básicos de los filtros de E/S son:

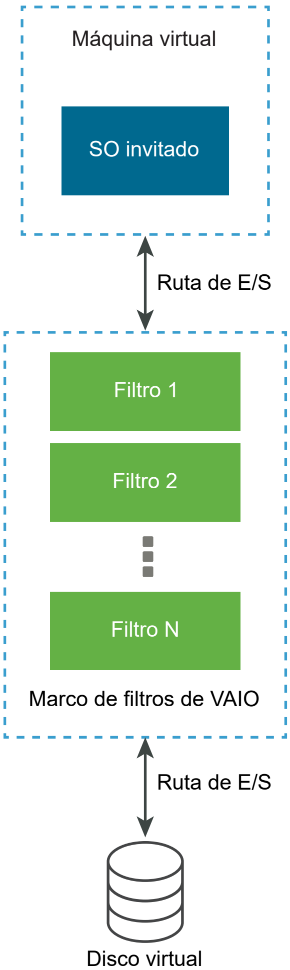
Marco de filtros de VAIO

Una combinación del ámbito del usuario y la infraestructura de VMkernel que proporciona ESXi. Con el marco, puede agregar complementos de filtro a la ruta de acceso de E/S hacia los discos virtuales y desde estos. La infraestructura incluye un proveedor de almacenamiento de filtro de E/S (proveedor VASA). El proveedor se integra con el sistema de administración de almacenamiento basada en directivas (Storage Policy Based Management, SPBM) y exporta las capacidades de filtro a vCenter Server.

Complemento de filtro de E/S

Un componente de software proporcionado por VMware o desarrollado por partners de VMware que intercepta y filtra los datos de E/S en tránsito entre los discos virtuales y los sistemas operativos invitados. Si los socios de VMware desarrollan los filtros de E/S, el filtro puede incluir componentes opcionales adicionales como ayuda para su configuración y administración.

La siguiente imagen muestra los componentes de los filtros de E/S y el flujo de E/S entre los sistemas operativos invitados y el disco virtual.



Cada componente ejecutable de máquina virtual (VMX) contiene un marco de filtro que administra los complementos de filtro de E/S conectados al disco virtual. El marco de filtro invoca los filtros cuando las solicitudes de E/S se transfieren entre el sistema operativo invitado y el disco virtual. Además, el filtro intercepta cualquier acceso de E/S hacia el disco virtual que sucede fuera de una máquina virtual en ejecución.

Los filtros se ejecutan de forma secuencial en un orden específico. Por ejemplo, un filtro de replicación se ejecuta antes que un filtro de memoria caché. Pueden funcionar varios filtros en el disco virtual, pero solo uno por categoría.

Una vez que todos los filtros del disco en particular comprueban la solicitud de E/S, la solicitud se transfiere a su destino, ya sea la máquina virtual o el disco virtual.

Dado que los filtros se ejecutan en un espacio de usuario, cualquier error de filtro solamente afecta a la máquina virtual, pero no afecta al host ESXi.

Proveedores de almacenamiento para filtros de E/S

Cuando se instalan filtros de E/S en hosts ESXi, el marco de filtros de E/S configura y registra un proveedor de almacenamiento, también llamado proveedor VASA, para cada host del clúster.

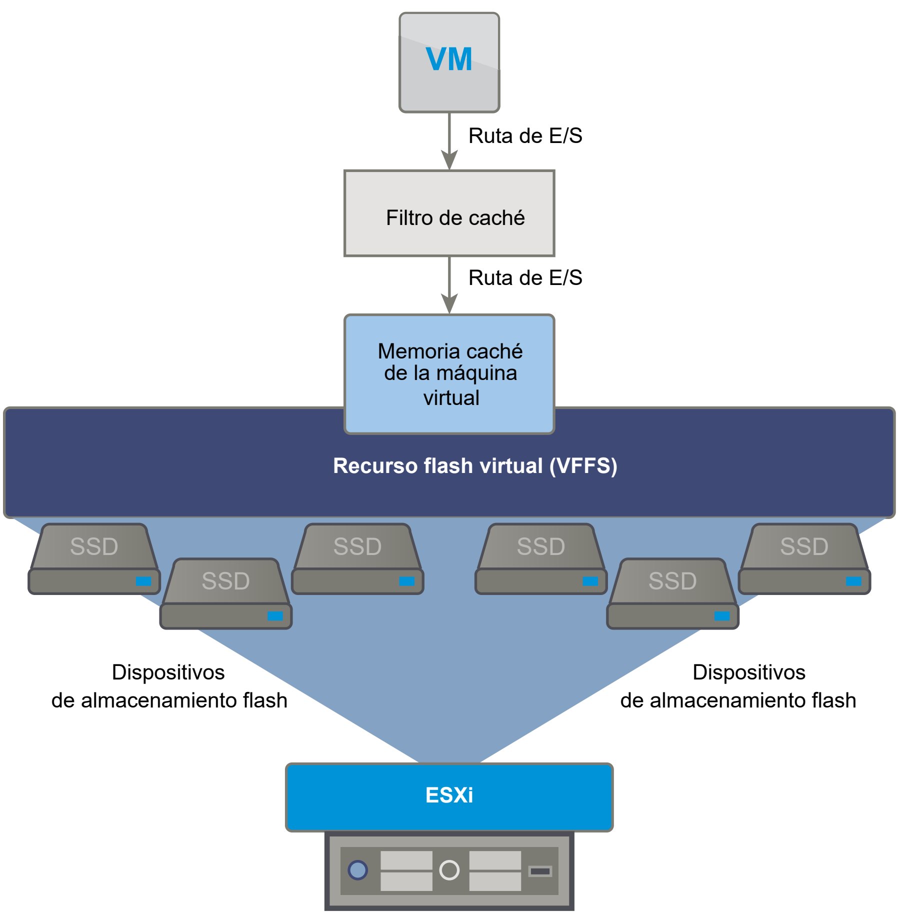
Los proveedores de almacenamiento de filtrado de E/S son componentes de software que ofrece vSphere. Estos se integran con los filtros de E/S e indican las capacidades de servicio de datos que los filtros de E/S admiten en vCenter Server.

Estas capacidades rellenan la interfaz de directivas de almacenamiento de máquina virtual y pueden incluirse en referencias de una directiva de almacenamiento de máquina virtual. Luego, se aplica la directiva a los discos virtuales para que los filtros de E/S puedan procesar las actividades de E/S en los discos.

Utilizar dispositivos de almacenamiento flash con filtros de E/S de memoria caché

Un filtro de E/S de memoria caché puede utilizar dispositivos de almacenamiento flash local para almacenar en caché los datos de la máquina virtual.

Si el filtro de E/S de almacenamiento en caché utiliza dispositivos flash locales, debe configurar un recurso flash virtual, también conocido como volumen VFFS. Antes de activar el filtro, debe configurar el recurso en su host ESXi. Mientras se procesan las operaciones de E/S de lectura de la máquina virtual, el filtro crea una memoria caché de la máquina virtual y la coloca en el volumen VFFS.



Para configurar un recurso flash virtual, se deben utilizar dispositivos flash conectados al host. Para aumentar la capacidad del recurso flash virtual, puede agregar más unidades flash. Una unidad flash individual debe estar asignada exclusivamente al recurso flash virtual y no puede compartirse con ningún otro servicio de vSphere, como vSAN o VMFS. Consulte Configurar un recurso flash virtual.

Requisitos del sistema para los filtros de E/S

Para poder usar los filtros de E/S en su entorno, debe cumplir ciertos requisitos específicos.

Se aplican los siguientes requisitos.

- Se debe utilizar la versión más reciente de ESXi y vCenter Server compatible con los filtros de E/S. En algunos casos, las versiones anteriores no admiten los filtros de E/S o solo ofrecen compatibilidad parcial.
- Consulte los requisitos adicionales de las soluciones de algunos partners. En algunos casos específicos, se necesitan dispositivos flash, memoria física adicional o conectividad de red y ancho de banda en el entorno. Para obtener información, comuníquese con el proveedor o el representante de VMware.
- Servidor web para usar como host de los paquetes de partners en la instalación de filtros. El servidor debe estar disponible después de la instalación inicial. Cuando un nuevo host se une al clúster, el servidor transfiere los componentes de filtro de E/S correspondientes al host.

Configurar filtros de E/S en el entorno de vSphere

Si desea configurar los servicios de datos que proporcionan los filtros de E/S para sus máquinas virtuales, debe seguir varios pasos.

Requisitos previos

- Cree un clúster que incluya al menos un host ESXi.
- Para obtener información acerca de los filtros de E/S suministrados por terceros, póngase en contacto con su proveedor o representante de VMware.

Procedimiento

1 Instalar filtros de E/S en un clúster

   Si usa filtros de E/S suministrados por terceros, instale los filtros de E/S en un clúster de hosts ESXi.

2 Ver filtros de E/S y proveedores de almacenamiento

   Utilice vSphere Client para revisar los filtros de E/S disponibles en el entorno y comprobar que los proveedores de dichos filtros se muestren según lo esperado y estén activos.

Instalar filtros de E/S en un clúster

Si usa filtros de E/S suministrados por terceros, instale los filtros de E/S en un clúster de hosts ESXi.

Los partners de VMware crean los filtros de E/S a través del programa de desarrolladores vSphere APIs for I/O Filtering (VAIO).

Los paquetes de filtro se distribuyen como paquetes ZIP del paquete de soluciones que pueden incluir daemons de filtro de E/S, bibliotecas de filtros de E/S, proveedores de CIM y otros componentes asociados.

Generalmente, para implementar los filtros, se ejecutan los instaladores suministrados por los proveedores. La instalación se realiza en el nivel del clúster ESXi. No se pueden instalar los filtros en los hosts seleccionados directamente.

Nota Si tiene pensado instalar filtros de E/S en el clúster de vSphere 7.0 y versiones posteriores, el clúster no puede incluir hosts ESXi 6.x. Los filtros compilados con el programa de vSphere 6.x VAIO no pueden funcionar en los hosts ESXi 7.0 y versiones posteriores porque el proveedor de CIM es de 32 bits en ESXi 6.x y de 64-bit en ESXi 7.0 y versiones posteriores. A su vez, los filtros compilados con el programa VAIO de vSphere 7.0 y versiones posteriores no son compatibles con los hosts ESXi 6.x.

Requisitos previos

- Privilegios necesarios: **Host.Configuración.Consultar revisión**.
- Compruebe que la solución de filtro de E/S esté certificada por VMware.

Procedimiento

- ◆ Ejecute el instalador que proporcionó el proveedor.

  El instalador implementa la extensión de filtros de E/S adecuada en vCenter Server y los componentes de filtro en todos los hosts de un clúster.

  El proveedor de almacenamiento, también denominado proveedor VASA, se registra automáticamente para cada host ESXi en el clúster. El correcto registro automático de los proveedores de almacenamiento de filtros de E/S activa un evento en el nivel del host. Si no es posible registrar automáticamente los proveedores de almacenamiento, el sistema emite alarmas en los hosts.

Ver filtros de E/S y proveedores de almacenamiento

Utilice vSphere Client para revisar los filtros de E/S disponibles en el entorno y comprobar que los proveedores de dichos filtros se muestren según lo esperado y estén activos.

Al instalar un filtro de E/S de terceros, se registra automáticamente un proveedor de almacenamiento, también denominado proveedor VASA, para cada host ESXi en el clúster. El correcto registro automático de los proveedores de almacenamiento de filtros de E/S activa un evento en el nivel del host. Si no es posible registrar automáticamente los proveedores de almacenamiento, el sistema emite alarmas en los hosts.

Procedimiento

1 Compruebe que los proveedores de almacenamiento de filtros de E/S se muestren según lo esperado y estén activos.

   a Desplácese hasta vCenter Server.

   b Haga clic en la pestaña **Configurar** y, a continuación, en **Proveedores de almacenamiento**.

   c Revise los proveedores de almacenamiento para comprobar los filtros de E/S.

   Una vez que los proveedores de filtros de E/S están registrados correctamente, la interfaz de directivas de almacenamiento de máquina virtual se rellena con las capacidades y los servicios de datos que ofrecen esos filtros.

2 Compruebe que los componentes del filtro de E/S se enumeren en el clúster y en los hosts ESXi.

Opción	Acciones
Ver filtros de E/S en un clúster	a Desplácese hasta el clúster. b Haga clic en la pestaña **Configurar**. c En **Configuración**, haga clic en **Filtros de E/S** para revisar los filtros instalados en el clúster.
Ver filtros de E/S en un host	a Desplácese hasta el host. b Haga clic en la pestaña **Configurar**. c En **Almacenamiento**, haga clic en **Filtros de E/S** para revisar los filtros instalados en el host.

Habilitar servicios de datos de filtros de E/S en discos virtuales

Habilitar los servicios de datos que ofrecen los filtros de E/S es un proceso bidireccional. Puede crear una directiva de máquina virtual en función de los servicios de datos que ofrecen los filtros de E/S; luego, puede asociar esta directiva a una máquina virtual.

Requisitos previos

Para los filtros de E/S de almacenamiento en caché, configure el recurso de flash virtual en el host ESXi antes de activar el filtro. Consulte Configurar un recurso flash virtual.

Procedimiento

1 Defina una directiva de máquina virtual en función de los servicios de filtro de E/S.

   Asegúrese de que la directiva de máquina virtual enumere los servicios de datos proporcionados por los filtros de E/S.

   Consulte Crear una directiva de almacenamiento de máquina virtual para los servicios de datos basados en host.

2 Asigne la directiva de filtros de E/S a una máquina virtual.

   Para activar los servicios de datos que proporciona el filtro de E/S, asocie la directiva de filtros de E/S con los discos virtuales. Puede asignar la directiva al aprovisionar la máquina virtual.

   Consulte Asignar la directiva de filtros de E/S a máquinas virtuales.

Pasos siguientes

Si más tarde desea deshabilitar el filtro de E/S para una máquina virtual, puede quitar las reglas del filtro de la directiva de almacenamiento de la máquina virtual y volver a aplicar la directiva. Consulte Editar o clonar una directiva de almacenamiento de máquina virtual. También puede editar la configuración de la máquina virtual y seleccionar una directiva de almacenamiento diferente que no incluya el filtro.

Asignar la directiva de filtros de E/S a máquinas virtuales

Para activar los servicios de datos que proporcionan los filtros de E/S, asocie la directiva de filtros de E/S con los discos virtuales. Puede asignar la directiva cuando crea o edita una máquina virtual.

Puede asignar la directiva de filtros de E/S durante la implementación inicial de una máquina virtual. Este tema describe cómo asignar la directa cuando se crea una máquina virtual nueva. Para obtener información sobre los métodos de implementación, consulte la documentación de *Administrar máquinas virtuales de vSphere*.

Nota No puede cambiar ni asignar la directiva de filtro de E/S cuando migra o clona una máquina virtual.

Requisitos previos

Compruebe que el filtro de E/S esté instalado en el host ESXi donde se ejecuta la máquina virtual.

Procedimiento

1 Inicie el proceso de aprovisionamiento de máquina virtual y siga los pasos adecuados.

2 Asigne la misma directiva de almacenamiento a todos los discos y archivos de máquina virtual.

   a En la página **Seleccionar almacenamiento**, seleccione una directiva de almacenamiento en el menú desplegable **Directiva de almacenamiento de máquina virtual**.

   b Seleccione el almacén de datos en la lista de almacenes de datos compatibles y haga clic en **Siguiente**.

      El almacén de datos se transforma en el recurso de almacenamiento de destino del archivo de configuración de la máquina virtual y de todos los discos virtuales. La directiva también activa los servicios de filtros de E/S para los discos virtuales.

3 Cambie la directiva de almacenamiento de máquina virtual del disco virtual.

   Use esta opción para habilitar filtros de E/S solo para sus discos virtuales.

   a En la página **Personalizar hardware**, expanda el panel **Disco duro nuevo**.

   b En el menú desplegable **Directiva de almacenamiento de máquina virtual**, seleccione la directiva de almacenamiento para asignar al disco virtual.

   c (opcional) Cambie la ubicación de almacenamiento del disco virtual.

      Use esta opción para almacenar el disco virtual en un almacén de datos distinto del almacén de datos en el que reside el archivo de configuración de máquina virtual.

4 Complete el proceso de aprovisionamiento de máquina virtual.

Resultados

Una vez creada la máquina virtual, la pestaña **Resumen** muestra las directivas de almacenamiento asignadas y su estado de cumplimiento.

Pasos siguientes

Posteriormente, puede cambiar la asignación de directiva virtual. Consulte Cambiar la asignación de directivas de almacenamiento para archivos y discos de máquinas virtuales.

Administrar filtros de E/S

Es posible ejecutar el instalador que el proveedor ofrece para instalar, desinstalar o actualizar los filtros de E/S.

Al trabajar con filtros de E/S, se deben tener en cuenta las siguientes consideraciones:

- vCenter Server utiliza ESX Agent Manager (EAM) para instalar y desinstalar filtros de E/S. Como administrador, nunca invoque las API de EAM directamente para agencias de EAM que vCenter Server crea o utiliza. Todas las operaciones relacionadas con los filtros de E/S deben pasar por las API de VIM. Si se modifica de forma accidental una agencia de EAM que vCenter Server creó, se deben revertir los cambios. Si se destruye por accidente la agencia de EAM que utilizan los filtros de E/S, se debe llamar a `Vim.IoFilterManager#uninstallIoFilter` para que se desinstalen los filtros de E/S afectados. Cuando finalice la desinstalación, vuelva a reinstalar.

- Cuando un host nuevo se une al clúster que tiene filtros de E/S, los filtros instalados en el clúster se implementan en el host. vCenter Server registra el proveedor de almacenamiento de filtros de E/S del host. Todos los cambios que se realicen en el clúster se verán en la interfaz de directivas de almacenamiento de máquina virtual de vSphere Client.
- Cuando transfiere un host de un clúster o lo quita de vCenter Server, los filtros de E/S se desinstalan del host. vCenter Server elimina del registro al proveedor de almacenamiento de filtro de E/S.
- Al utilizar un host ESXi sin estado, es posible que el host pierda su VIB de filtros de E/S durante el reinicio. vCenter Server comprueba los paquetes instalados en el host después del reinicio y envía los VIB de filtros de E/S al host, de ser necesario.

Desinstalar filtros de E/S de un clúster

Puede desinstalar filtros de E/S implementados en un clúster de hosts ESXi.

Requisitos previos

- Privilegios necesarios:**Host.Config.Revisión**.

Procedimiento

1 Para desinstalar el filtro de E/S, ejecute el instalador que le proporcione su proveedor.

   Durante la desinstalación, un instalador de filtro de E/S de terceros coloca automáticamente los hosts en modo de mantenimiento.

   Si la desinstalación se realiza correctamente, el filtro y los componentes relacionados se quitan de los hosts.

2 Compruebe que los componentes del filtro de E/S se desinstalaron correctamente de los hosts ESXi. Utilice uno de los siguientes métodos:

   - Ejecute el comando `esxcli software vib list`.
   - Vea los filtros de E/S en vSphere Client. Consulte Ver filtros de E/S y proveedores de almacenamiento.

   El filtro desinstalado ya no aparece en la lista.

Actualizar filtros de E/S en un clúster

Después de actualizar los hosts ESXi a la versión 7.0 y versiones posteriores, use los instaladores proporcionados por los proveedores de filtros de E/S para actualizar los filtros de E/S implementados en el clúster de hosts ESXi.

Cuando actualiza un host ESXi 6.x que tiene VIB de filtro de E/S personalizados a la versión 7.0 y posterior, se migran todos los VIB personalizados compatibles. Sin embargo, los filtros de E/S heredados no pueden funcionar en ESXi 7.0 y versiones posteriores. Los filtros generalmente incluyen proveedores de CIM de 32 bits, mientras que ESXi 7.0 y versiones posteriores requieren aplicaciones de CIM de 64 bits. Debe actualizar los filtros heredados para que sean compatibles.

La actualización consiste en desinstalar los componentes de filtro anteriores y reemplazarlos por los nuevos componentes de filtro. Para determinar si una instalación es una actualización, vCenter Server comprueba los nombres y las versiones de los filtros existentes. Si los nombres de los filtros existentes coinciden con los nombres de los filtros nuevos, pero tienen versiones diferentes, se considera que la instalación es una actualización.

Requisitos previos

- Privilegios necesarios:**Host.Config.Revisión**.
- Actualice los hosts a ESXi 7.0 y versiones posteriores. Si utiliza vSphere Lifecycle Manager para la actualización, consulte la documentación de *Administración del ciclo de vida de hosts y clústeres*.

Procedimiento

1 Para actualizar el filtro, ejecute el instalador suministrado por el proveedor.

   Durante la actualización, un instalador de filtro de E/S externo automáticamente pone a los hosts en modo de mantenimiento.

   El instalador identifica todos los componentes de filtro existentes y los quita antes de instalar los nuevos componentes de filtro.

2 Compruebe si los componentes de filtro de E/S se instalaron correctamente en los hosts ESXi. Utilice uno de los siguientes métodos:

   - Ejecute el comando `esxcli software vib list`.
   - Vea los filtros de E/S en vSphere Client. Consulte Ver filtros de E/S y proveedores de almacenamiento.

Resultados

Después de la actualización, el sistema vuelve a colocar los hosts en modo operativo.

Directrices y prácticas recomendadas para los filtros de E/S

Al utilizar filtros de E/S en el entorno, siga las instrucciones y las prácticas recomendadas específicas.

- Dado que los filtros de E/S son independientes del almacén de datos, todos los tipos de almacenes de datos, incluidos VMFS, NFS, Virtual Volumes y vSAN, son compatibles con los filtros de E/S.
- Los filtros de E/S admiten RDM en el modo de compatibilidad virtual. No se admiten RDM en el modo de compatibilidad física.
- No puede cambiar ni asignar la directiva de filtro de E/S mientras migra o clona una máquina virtual. Puede cambiarla después de finalizar la migración o la clonación.

- Al clonar o migrar una máquina virtual con una directiva de filtro de E/S de un host a otro, asegúrese de que el host de destino tenga instalado un filtro compatible. Este requisito se aplica a las migraciones que inician un administrador o funciones como HA o DRS.
- Al convertir una plantilla en una máquina virtual, si la plantilla está configurada con una directiva de filtro de E/S, el host de destino debe tener el filtro de E/S compatible instalado.
- Si utiliza vCenter Site Recovery Manager para replicar discos virtuales, los discos que se obtienen en el sitio de recuperación no tienen directivas de filtro de E/S. Debe crear estas directivas de filtro de E/S en el sitio de recuperación y volver a asociarlas a los discos replicados.
- Si la máquina virtual tiene un árbol de instantáneas asociado, no se puede agregar, cambiar ni quitar la directiva de filtro de E/S para la máquina virtual.

Migrar máquinas virtuales con filtros de E/S

Al migrar una máquina virtual con filtros de E/S, existen consideraciones específicas que se deben tener en cuenta.

Si se utiliza Storage vMotion para migrar una máquina virtual con filtros de E/S, debe conectarse un almacén de datos de destino a los hosts con filtros de E/S compatibles instalados.

Es posible que deba migrar una máquina virtual con filtros de E/S en distintos tipos de almacenes de datos, por ejemplo, entre VMFS y Virtual Volumes. En tal caso, asegúrese de que la directiva de almacenamiento de máquina virtual incluya conjuntos de reglas para cada tipo de almacén de datos que planea utilizar. Por ejemplo, si se migra la máquina virtual entre almacenes de datos de VMFS y Virtual Volumes, cree una directiva de almacenamiento de máquina virtual mixta que incluya las siguientes reglas:

- Reglas comunes para los filtros de E/S.
- Conjunto de reglas 1 para el almacén de datos de VMFS. Debido a que la administración de almacenamiento basada en directivas no ofrece una directiva de VMFS explícita, el conjunto de reglas debe incluir las reglas basadas en etiquetas para el almacén de datos de VMFS.
- Conjunto de reglas 2 para el almacén de datos de Virtual Volumes

Cuando Storage vMotion migra la máquina virtual, se selecciona el conjunto de reglas correcto que corresponde al almacén de datos de destino. Las reglas de filtros de E/S se mantienen iguales.

Si no especifica reglas para los almacenes de datos y únicamente define reglas comunes para los filtros de E/S, el sistema aplica las directivas de almacenamiento predeterminadas para los almacenes de datos.

Controlar errores de instalación de filtros de E/S

En general, todos los hosts ESXi de un clúster tienen el mismo conjunto de filtros de E/S instalado. En ocasiones, pueden generarse errores durante la instalación.

Si se produce un error en la instalación de un filtro de E/S en un host, el sistema genera eventos que informan acerca del error. Además, una alarma en el host muestra el motivo del error. A continuación se proporcionan ejemplos de errores:

- No se puede obtener acceso a la URL de VIB desde el host.
- El VIB tiene un formato no válido.
- El VIB requiere que el host esté en modo de mantenimiento para ejecutar una actualización o una desinstalación.
- El VIB requiere que el host se reinicie después de ejecutar la instalación o la desinstalación.
- Los intentos para que el host entre en el modo de mantenimiento producen errores porque no se puede evacuar la máquina virtual desde el host.
- El VIB requiere una instalación o una desinstalación manuales.

vCenter Server puede solucionar algunos errores. Es posible que deba intervenir si se generan otros errores. Por ejemplo, es posible que deba editar la URL de VIB, evacuar o apagar las máquinas virtuales de forma manual, o bien instalar o desinstalar los VIB de forma manual.

Instalar filtros de E/S en un único host ESXi

A los fines de solución de problemas, puede descargar un componente de ESXi del filtro de E/S, en un paquete como archivo VIB, e instalarlo en el host ESXi. Utilice el comando `esxcli` para instalar el archivo VIB.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 Instale VIB al ejecutar el siguiente comando:

   `esxcli software vib install --depot` ***`path_to_VMware_vib_ZIP_file`***

   Las opciones del comando `install` permiten realizar un simulacro, especificar un VIB, omitir la comprobación del nivel de aceptación, etc. No omita la comprobación en los sistemas de producción. Consulte la documentación de *Referencia de ESXCLI*.

2 Compruebe que los VIB estén instalados en el host ESXi.

   `esxcli software vib list`

Aceleración de hardware de almacenamiento 24

La funcionalidad de aceleración de hardware permite que el host ESXi se integre con sistemas de almacenamiento compatibles. El host puede descargar ciertas operaciones de administración de máquina virtual y almacenamiento en los sistemas de almacenamiento. Con la asistencia de hardware de almacenamiento, el host realiza estas operaciones más rápidamente y consume menos CPU, memoria y ancho de banda de tejido de almacenamiento.

Los dispositivos de almacenamiento en bloque, canal de fibra y de iSCSI, y los dispositivos NAS admiten la aceleración de hardware.

Para obtener detalles adicionales, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/1021976.

Este capítulo incluye los siguientes temas:

Beneficios de la aceleración de hardware

Cuando se admite la funcionalidad de aceleración de hardware, el host puede obtener asistencia de hardware y realizar varias tareas de forma más rápida y eficaz.

El host puede obtener asistencia en las actividades siguientes:

- Migrar máquinas virtuales con Storage vMotion
- Implementar máquinas virtuales desde plantillas
- Clonar máquinas virtuales o plantillas
- Bloquear clústeres de VMFS y operaciones de metadatos para archivos de máquina virtual
- Aprovisionar discos virtuales gruesos
- Crear máquinas virtuales con tolerancia a errores

- Crear y clonar discos gruesos en almacenes de datos de NFS

Requisitos de aceleración de hardware

La funcionalidad de aceleración de hardware solo funciona si se utiliza una combinación adecuada de host y matriz de almacenamiento.

Tabla 24-1. Requisitos de almacenamiento de aceleración de hardware

ESXi	Dispositivos de almacenamiento en bloque	Dispositivos NAS
ESXi	Compatibilidad con el estándar T10 SCSI o complementos de almacenamiento en bloque para integración de matrices (VAAI)	Compatibilidad con complementos NAS para integración de matrices

Nota Si el tejido de almacenamiento SAN o NAS utiliza un dispositivo intermedio frente a un sistema de almacenamiento compatible con la aceleración de hardware, este dispositivo también debe ser compatible con la aceleración de hardware y contar con las certificaciones apropiadas. El dispositivo intermedio puede ser un dispositivo de virtualización de almacenamiento, de aceleración de E/S, de cifrado, etc.

Estado de compatibilidad con la aceleración de hardware

vSphere Client muestra el estado de compatibilidad con aceleración de hardware de cada dispositivo de almacenamiento y almacén de datos.

Los valores de estado son Desconocido, Compatible y No compatible. El valor inicial es Unknown.

En el caso de los dispositivos en bloque, el estado cambia a Supported después de que el host finaliza correctamente la operación de descarga. Si la operación de descarga genera errores, el estado cambia a Not Supported. El estado permanece como Unknown si el dispositivo ofrece una compatibilidad parcial con la aceleración de hardware.

Con NAS, el estado cambia a Supported cuando el almacenamiento puede realizar al menos una operación de descarga de hardware.

Cuando los dispositivos de almacenamiento no son compatibles u ofrecen compatibilidad parcial con las operaciones del host, el host vuelve a los métodos nativos para realizar las operaciones no admitidas.

Aceleración de hardware para dispositivos de almacenamiento en bloque

Con la aceleración de hardware, el host puede integrarse con dispositivos de almacenamiento en bloque, canal de fibra o iSCSI, y utilizar ciertas operaciones de matriz de almacenamiento.

La aceleración de hardware de ESXi admite las siguientes operaciones de matriz:

- Copia completa, también conocida como bloques de clonación o descarga de copias. Permite a las matrices de almacenamiento realizar copias completas de datos dentro de la matriz sin hacer que el host lea y escriba la información. Esta operación disminuye el tiempo y la carga de red cuando se clonan máquinas virtuales, se ejecuta el aprovisionamiento desde una plantilla o se realizan migraciones con vMotion.
- Puesta a cero de bloques, que también se conoce como escribir lo mismo. Permite que las matrices de almacenamiento pongan a cero una gran cantidad de bloques para proporcionar almacenamiento asignado recientemente, libre de datos escritos anteriormente. Esta operación disminuye el tiempo y la carga de red cuando crea máquinas virtuales y da formato a discos virtuales.
- Bloqueo asistido por hardware, también denominado prueba y configuración atómica (ATS). Admite el bloqueo discreto de máquinas virtuales sin utilizar reservas de SCSI. Esta operación permite el bloqueo de discos por sector, en lugar del LUN completo como con reservas de SCSI.

Compruebe con el proveedor la compatibilidad con la aceleración de hardware. Ciertas matrices de almacenamiento requieren que se active la compatibilidad del lado del almacenamiento.

En el host, la aceleración de hardware está habilitada de forma predeterminada. Si el almacenamiento no admite la aceleración de hardware, es posible deshabilitarla.

Además de la compatibilidad con la aceleración de hardware, ESXi admite el aprovisionamiento fino de matrices. Para obtener información, consulte ESXi y aprovisionamiento fino de matrices.

Deshabilitar la aceleración de hardware para dispositivos de almacenamiento en bloque

En el host, la aceleración de hardware para dispositivos de almacenamiento en bloque está habilitada de forma predeterminada. Se puede utilizar la configuración avanzada de vSphere Client para deshabilitar las operaciones de aceleración de hardware.

Como con cualquier opción de configuración avanzada, antes de deshabilitar la aceleración de hardware, consulte al equipo de soporte de VMware.

Procedimiento

1. En vSphere Client, desplácese hasta el host ESXi.
2. Haga clic en la pestaña **Configurar**.
3. En **Sistema**, haga clic en **Configuración avanzada del sistema**.
4. Cambie el valor de cualquiera de las opciones a 0 (deshabilitado):
   - VMFS3.HardwareAcceleratedLocking
   - DataMover.HardwareAcceleratedMove
   - DataMover.HardwareAcceleratedInit

Administrar aceleración de hardware en dispositivos de almacenamiento en bloque

Para integrarse con las matrices de almacenamiento de bloques, vSphere utiliza las extensiones de ESXi llamadas Storage APIs - Array Integration (VAAI). Con esta integración, vSphere puede utilizar las operaciones de hardware de la matriz.

En vSphere 5.x y versiones posteriores, estas extensiones se implementan como comandos T10 SCSI. En consecuencia, en dispositivos compatibles con el estándar T10 SCSI, el host ESXi puede comunicarse directamente y no requiere los complementos de VAAI.

Si el dispositivo no es compatible con T10 SCSI o proporciona compatibilidad parcial, ESXi utilizará los complementos VAAI instalados en el host. El host también puede usar una combinación de los comandos y los complementos T10 SCSI. Los complementos de VAAI son específicos de cada proveedor y pueden ser desarrollados por VMware o por un partner. Para administrar el dispositivo compatible con VAAI, el host asocia al dispositivo el filtro VAAI y el complemento VAAI específico del proveedor.

Para saber si el almacenamiento requiere complementos de VAAI o es compatible con la aceleración de hardware a través de los comandos T10 SCSI, consulte la *Guía de compatibilidad de VMware* o póngase en contacto con el proveedor de almacenamiento.

Es posible utilizar varios comandos `esxcli` para consultar dispositivos de almacenamiento y acceder a la información de compatibilidad de aceleración de hardware. Para los dispositivos que requieren los complementos de VAAI, también están disponibles los comandos de reglas de notificación. Para obtener información sobre los comandos `esxcli`, consulte *Introducción a ESXCLI*.

Mostrar los complementos y el filtro de aceleración de hardware

Para comunicarse con los dispositivos que no son compatibles con el estándar T10 SCSI, el host utiliza un único filtro VAAI y un complemento VAAI específico del proveedor. Utilice el comando `esxcli` para ver el filtro de aceleración de hardware y los complementos cargados actualmente en el sistema.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

- Ejecute el comando **`esxcli storage core plugin list --plugin-class=`*`value`***.

  En *value*, escriba uno de los siguientes parámetros:

  - Escriba `VAAI` para mostrar los complementos.

El resultado de este comando es similar al ejemplo siguiente:

```
#esxcli storage core plugin list --plugin-class=VAAI
Plugin name         Plugin class
VMW_VAAIP_EQL       VAAI
VMW_VAAIP_NETAPP    VAAI
VMW_VAAIP_CX        VAAI
```

- Escriba `Filter` para mostrar el filtro.

  El resultado de este comando es similar al ejemplo siguiente:

```
esxcli storage core plugin list --plugin-class=Filter
Plugin name  Plugin class
VAAI_FILTER  Filter
```

Comprobar el estado de compatibilidad de la aceleración de hardware

Use el comando `esxcli` para comprobar el estado de compatibilidad de la aceleración de hardware de un determinado dispositivo de almacenamiento.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

- Ejecute el comando **`esxcli storage core device list -d=`*`device_ID`***.

  La salida mostrará el estado de aceleración de hardware, o VAAI, que puede ser desconocido, compatible o no compatible.

```
# esxcli storage core device list -d naa.XXXXXXXXXXXX4c
naa.XXXXXXXXXXXX4c
 Display Name: XXXX Fibre Channel Disk(naa.XXXXXXXXXXXX4c)
 Size: 20480
 Device Type: Direct-Access
 Multipath Plugin: NMP
 XXXXXXXXXXXXXXXX
 Attached Filters: VAAI_FILTER
 VAAI Status: supported
 XXXXXXXXXXXXXXXX
```

Comprobar los detalles de compatibilidad con la aceleración de hardware

Use el comando `esxcli` para consultar si el dispositivo de almacenamiento en bloque proporciona compatibilidad con la aceleración de hardware.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

- Ejecute el comando **esxcli storage core device vaai status get -d=*device_ID***.

  Si un complemento VAAI administra el dispositivo, el resultado muestra el nombre del complemento asociado al dispositivo. La salida también muestra el estado de compatibilidad de cada T10 SCSI primitivo, si están disponibles. En el siguiente ejemplo se muestra una salida:

```
# esxcli storage core device vaai status get -d naa.XXXXXXXXXXXX4c
naa.XXXXXXXXXXXX4c
 VAAI Plugin Name: VMW_VAAIP_SYMM
 ATS Status: supported
 Clone Status: supported
 Zero Status: supported
 Delete Status: unsupported
```

Lista de reglas de notificación de aceleración de hardware

Cada dispositivo de almacenamiento en bloque administrado por un complemento VAAI necesita dos reglas de notificación. Una regla de notificación especifica el filtro de aceleración de hardware; la otra especifica el complemento de aceleración de hardware para el dispositivo. Se pueden utilizar los comandos `esxcli` para generar una lista de las reglas de notificación del filtro y del complemento de aceleración de hardware.

Procedimiento

1 Para generar una lista de las reglas de notificación de filtro, ejecute el comando **esxcli storage core claimrule list --claimrule-class=Filter**.

  En este ejemplo, las reglas de notificación de filtro especifican los dispositivos que notifica el filtro VAAI_FILTER.

```
# esxcli storage core claimrule list --claimrule-class=Filter
Rule Class   Rule   Class   Type   Plugin      Matches                    XCOPY Use Array
Reported Values  XCOPY Use Multiple Segments  XCOPY Max Transfer Size KiB
Filter       65430  runtime vendor VAAI_FILTER
vendor=EMC model=SYMMETRIX                           False
False                           0
Filter       65430  file    vendor VAAI_FILTER
vendor=EMC model=SYMMETRIX                           False
False                           0
Filter       65431  runtime vendor VAAI_FILTER
vendor=DGC model=*                                   False
False                           0
Filter       65431  file    vendor VAAI_FILTER
vendor=DGC model=*                                   False
False                           0
```

2 Para generar una lista de las reglas de notificación del complemento VAAI, ejecute el comando **esxcli storage core claimrule list --claimrule-class=VAAI**.

En este ejemplo, las reglas de notificación de VAAI especifican los dispositivos que notifica el complemento VAAI.

```
esxcli storage core claimrule list --claimrule-class=VAAI
Rule Class   Rule   Class   Type    Plugin         Matches                  XCOPY Use
Array Reported Values  XCOPY Use Multiple Segments  XCOPY Max Transfer Size KiB
VAAI         65430  runtime vendor  VMW_VAAIP_SYMM
vendor=EMC model=SYMMETRIX                          False
False                         0
VAAI         65430  file    vendor  VMW_VAAIP_SYMM
vendor=EMC model=SYMMETRIX                          False
False                         0
VAAI         65431  runtime vendor  VMW_VAAIP_CX
vendor=DGC model=*                                  False
False                         0
VAAI         65431  file    vendor  VMW_VAAIP_CX
vendor=DGC model=*                                  False
False                         0
```

Agregar reglas de notificación de aceleración de hardware

A fin de configurar la aceleración de hardware para una nueva matriz, agregue dos reglas de notificación, una para el filtro VAAI y otra para el complemento VAAI. Para que las nuevas reglas de notificación estén activas, primero se deben definir las reglas y, a continuación, cargarlas en el sistema.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 Defina una regla de notificación nueva para el filtro VAAI. Para ello, ejecute el comando **esxcli storage core claimrule add --claimrule-class=Filter --plugin=VAAI_FILTER**.

2 Defina una regla de notificación nueva para el complemento VAAI. Para ello, ejecute el comando **esxcli storage core claimrule add --claimrule-class=VAAI**.

3 Cargue ambas reglas de notificación ejecutando los comandos siguientes:

esxcli storage core claimrule load --claimrule-class=Filter

esxcli storage core claimrule load --claimrule-class=VAAI

4 Ejecute la regla de notificación de filtro VAAI con el comando **esxcli storage core claimrule run --claimrule-class=Filter**.

> **Nota** Solo se deben ejecutar las reglas de clase de filtro. Cuando el filtro VAAI reclama un dispositivo, encuentra automáticamente el complemento VAAI adecuado para asociar.

Ejemplo: Definir reglas de notificación de aceleración de hardware

Este ejemplo muestra cómo configurar la aceleración de hardware para matrices de IBM con el complemento VMW_VAAIP_T10. Utilice la siguiente secuencia de comandos. Para obtener información sobre las opciones que acepta el comando, consulte Agregar reglas de notificación de múltiples rutas.

```
# esxcli storage core claimrule add --claimrule-class=Filter --
plugin=VAAI_FILTER --type=vendor --vendor=IBM --autoassign
```

```
# esxcli storage core claimrule add --claimrule-class=VAAI --
plugin=VMW_VAAIP_T10 --type=vendor --vendor=IBM --autoassign
```

```
# esxcli storage core claimrule load --claimrule-class=Filter
```

```
# esxcli storage core claimrule load --claimrule-class=VAAI
```

```
# esxcli storage core claimrule run --claimrule-class=Filter
```

Configurar parámetros de XCOPY

XCOPY es un comando primitivo de VAAI que se utiliza para la descarga de tareas en la matriz de almacenamiento. Por ejemplo, puede utilizar XCOPY para descargar operaciones como la migración o la clonación de máquinas virtuales en la matriz en vez de consumir recursos de vSphere para realizar estas tareas.

Puede utilizar el mecanismo XCOPY con todas las matrices de almacenamiento que admiten el complemento VMW_VAAIP_T10 basado en SCSI T10 desarrollado por VMware. Para habilitar el mecanismo XCOPY, cree una regla de notificación de la clase VAAI.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

- Utilice el siguiente comando y especifique las opciones de XCOPY:

  ```
  esxcli storage core claimrule add --claimrule-class=VAAI
  ```

Para obtener información sobre las opciones que acepta el comando, consulte Agregar reglas de notificación de múltiples rutas.

Opción	Descripción
-a|--xcopy-use-array-values	Se utilizan valores que la matriz informa para los comandos XCOPY.
-s|--xcopy-use-multi-segs	Se utilizan varios segmentos para los comandos XCOPY. Válido únicamente cuando se especifica `--xcopy-use-array-values`.
-m|--xcopy-max-transfer-size	Tamaño máximo de transferencia en MB para los comandos XCOPY cuando se utiliza un tamaño de transferencia diferente al informado por la matriz. Válido únicamente cuando se especifica `--xcopy-use-array-values`.
-k|--xcopy-max-transfer-size-kib	Tamaño máximo de transferencia en KiB para los comandos XCOPY cuando se utiliza un tamaño de transferencia diferente al informado por la matriz. Válido únicamente si se especifica `--xcopy-use-array-values`.

Ejemplo: Configuración de XCOPY

- ```
  # esxcli storage core claimrule add -r 914 -t vendor -V XtremIO -M XtremApp -P
  VMW_VAAIP_T10 -c VAAI -a -s -k 64
  ```

- ```
  # esxcli storage core claimrule add -r 65430 -t vendor -V EMC -M SYMMETRIX -P
  VMW_VAAIP_SYMM -c VAAI -a -s -m 200
  ```

Eliminar reglas de notificación de aceleración de hardware

Utilice el comando `esxcli` para eliminar las reglas de notificación de aceleración de hardware existentes.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

◆ Ejecute los siguientes comandos:

`esxcli storage core claimrule remove -r claimrule_ID --claimrule-class=Filter`

`esxcli storage core claimrule remove -r claimrule_ID --claimrule-class=VAAI`

Aceleración de hardware en dispositivos NAS

Con la aceleración de hardware, los hosts ESXi se integran con dispositivos NAS y usan varias operaciones de hardware que proporciona el almacenamiento NAS. La aceleración de hardware utiliza vSphere API for Array Integration (VAAI) para facilitar la comunicación entre los hosts y los dispositivos de almacenamiento.

El marco NAS de VAAI es compatible con ambas versiones de almacenamiento NFS: NFS 3 y NFS 4.1.

El NAS de VAAI utiliza un conjunto de primitivos de almacenamiento para descargar las operaciones de almacenamiento desde el host hasta la matriz. La lista siguiente muestra las operaciones NAS admitidas:

Clonación completa de archivos

Admite una capacidad de dispositivo NAS para clonar archivos del disco virtual. Esta operación es similar a la clonación en bloque de VMFS, a excepción de que los dispositivos NAS clonan archivos completos en lugar de segmentos de archivos. Las tareas que se benefician de la operación de clonación de archivos completa son la clonación de máquinas virtuales, Storage vMotion y la implementación de máquinas virtuales a partir de plantillas.

Cuando el host ESXi copia los datos con VAAI NAS, no necesita leer los datos de NAS y volver a escribir los datos en NAS. El host simplemente envía el comando de copia para descargarlo en NAS. El proceso de copia se realiza en NAS, lo que reduce la carga en el host.

Clonación rápida de archivos

Esta operación, también conocida como instantáneas nativas o basadas en matrices, descarga la creación de instantáneas de máquinas virtuales y clones vinculados en la matriz.

Reserva de espacio

Admite una capacidad de matrices de almacenamiento para asignar espacio para un archivo de disco virtual en el formato grueso.

Generalmente, cuando crea un disco virtual en un almacén de datos NFS, el servidor NAS determina la directiva de asignación. La directiva de asignación predeterminada en la mayoría de los servidores NAS es de formato fino y no garantiza la copia de seguridad del almacenamiento en el archivo. Sin embargo, la operación de reserva de espacio puede indicar al dispositivo NAS que utilice mecanismos específicos del proveedor para reservar espacio para un disco virtual. Como resultado, se pueden crear discos virtuales gruesos en el almacén de datos NFS si el servidor NAS de respaldo es compatible con la operación de reserva de espacio.

Estadísticas ampliadas

Admite la visibilidad del uso del espacio en dispositivos NAS. La operación permite consultar los detalles de uso de espacio de los discos virtuales en almacenes de datos de NFS. Los detalles incluyen el tamaño de un disco virtual y el consumo de espacio de este. Esta funcionalidad resulta útil para el aprovisionamiento fino.

Con los dispositivos de almacenamiento NAS, la integración con la aceleración de hardware se implementa a través de complementos NAS específicos del proveedor. Generalmente, los proveedores crean estos complementos, y se distribuyen como paquetes de proveedores. No se necesitan reglas de notificación para que funcionen los complementos NAS.

Están disponibles varias herramientas para instalar y actualizar complementos de NAS. Incluyen los comandos `esxcli` y vSphere Lifecycle Manager. Para obtener más información, consulte la documentación de *Actualizar VMware ESXi* y *Administración del ciclo de vida de hosts y clústeres*. Para conocer las recomendaciones de instalación y actualización, consulte el artículo de la base de conocimientos.

Nota Los proveedores de almacenamiento de NAS pueden proporcionar opciones de configuración adicionales que pueden afectar el rendimiento y el funcionamiento de VAAI. Siga las recomendaciones del proveedor y configure las opciones adecuadas en la matriz de almacenamiento de NAS y ESXi. Consulte la documentación del proveedor de almacenamiento para obtener más información.

Habilitar instantáneas nativas de NAS en máquinas virtuales

Si la implementación incluye matrices NAS que admiten las API de vSphere para la integración de matrices (VAAI), puede usar la tecnología de clonación rápida de archivos, también denominada instantáneas NFS nativas, para crear instantáneas de máquinas virtuales. Con esta tecnología, el dispositivo NFS copia la máquina virtual sin que el host ESXi lea y escriba los datos. Esta operación puede reducir el tiempo y la carga de red cuando se crean instantáneas de máquina virtual.

De forma predeterminada, todas las máquinas virtuales creadas recientemente admiten la tecnología de instantáneas ESXi tradicionales. Para usar la tecnología de instantánea nativas NFS, habilite esta opción para la máquina virtual.

Requisitos previos

- Compruebe que la matriz NAS admita la operación de clonación rápida de archivos con el programa NAS de VAAI.
- En el host ESXi, instale el complemento NAS específico del proveedor que admite la clonación rápida de archivos con VAAI.
- Siga las recomendaciones del proveedor de almacenamiento NAS para configurar las opciones necesarias tanto en la matriz NAS como en ESXi. Consulte la documentación del proveedor de almacenamiento para obtener más información.

Procedimiento

1. En vSphere Client, haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.
2. Haga clic en la pestaña **Opciones de máquina virtual** y expanda el menú **Opciones avanzadas**.
3. Haga clic en **Editar configuración** junto a Parámetros de configuración.
4. Configure el parámetro **`snapshot.alwaysAllowNative`**.

   Si el parámetro existe, asegúrese de que su valor esté establecido como True. Si no existe, agréguelo y establezca su valor como True.

Nombre	Valor
snapshot.alwaysAllowNative	True

Consideraciones sobre la aceleración de hardware

Cuando se utiliza la funcionalidad de aceleración de hardware con ESXi, se aplican ciertas consideraciones.

Varios motivos pueden causar errores en una operación acelerada por hardware.

Por cada primitivo que la matriz no implementa, la matriz devuelve un error. El error activa el host ESXi para intentar la operación con los métodos nativos.

El administrador de transferencia de datos de VMFS no aprovecha las descargas de hardware, en su lugar, utiliza el movimiento de los datos de software cuando ocurre una de las situaciones siguientes:

- Los almacenes de datos de VMFS de origen y destino tienen distintos tamaños de bloques.
- El tipo de archivo de origen es RDM y el tipo de archivo de destino no lo es (archivo normal).
- El tipo VMDK de origen es grueso con todos los bloques puestos a cero y el tipo de VMDK de destino es fino.
- El VMDK de origen o destino está en formato disperso o alojado.
- La máquina virtual de origen tiene una snapshot.
- La dirección lógica y la longitud de transferencia en la operación solicitada no están alineadas con la alineación mínima que requiere el dispositivo de almacenamiento. Todos los almacenes de datos creados con vSphere Client se alinean automáticamente.
- VMFS tiene varios LUN o extensiones, y se encuentran en distintas matrices.

La clonación de hardware entre matrices, incluso dentro del mismo almacén de datos de VMFS, no funciona.

Aprovisionamiento de almacenamiento y recuperación de espacio

25

vSphere admite dos modelos de aprovisionamiento de almacenamiento: aprovisionamiento grueso y aprovisionamiento fino.

Aprovisionamiento grueso

Es un modelo tradicional de aprovisionamiento de almacenamiento. Con el aprovisionamiento grueso, se proporciona por adelantado una gran cantidad de espacio de almacenamiento para anticipar necesidades de almacenamiento futuras. Sin embargo, el espacio puede permanecer inutilizado, lo que genera la infrautilización de la capacidad de almacenamiento.

Aprovisionamiento fino

Este método se opone al aprovisionamiento grueso y ayuda a eliminar problemas de infrautilización del almacenamiento al asignar el espacio de almacenamiento de manera flexible y a petición. Con ESXi, puede usar dos modelos de aprovisionamiento fino: en el nivel de la matriz y en el nivel del disco virtual.

El aprovisionamiento fino permite informar más espacio de almacenamiento virtual que la capacidad física real. Esta discrepancia puede llevar a una sobresuscripción de almacenamiento, también denominada sobreaprovisionamiento. Cuando utilice aprovisionamiento fino, supervise el uso real del almacenamiento para evitar condiciones en las que se queda sin espacio de almacenamiento físico.

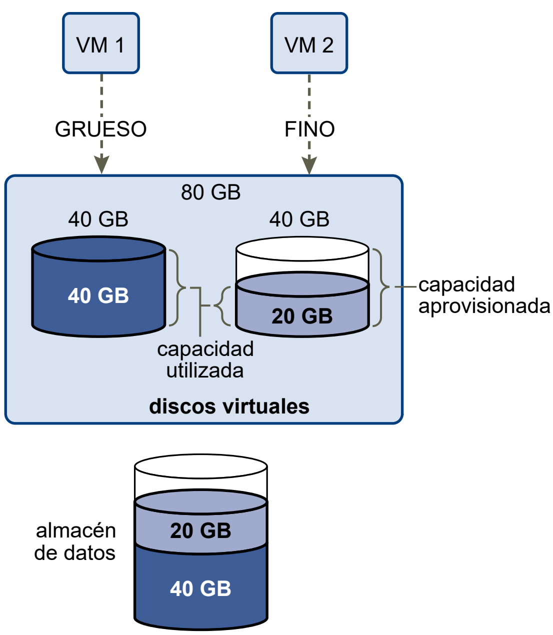
Este capítulo incluye los siguientes temas:

Aprovisionamiento fino de discos virtuales

Cuando se crea una máquina virtual, se aprovisiona una cierta cantidad de espacio de almacenamiento de un almacén de datos a archivos de disco virtual.

De forma predeterminada, ESXi ofrece un método de aprovisionamiento de almacenamiento tradicional para las máquinas virtuales. Con este método, primero se estima cuánto almacenamiento necesitará la máquina virtual para el ciclo de vida completo. A continuación, se aprovisiona una cantidad fija de espacio de almacenamiento para el disco virtual de VM por adelantado, por ejemplo, 40 GB. Todo el espacio aprovisionado se confirma en el disco virtual. Un disco virtual que inmediatamente ocupa todo el espacio aprovisionado es un disco grueso.

ESXi admite el aprovisionamiento fino de discos virtuales. Con la característica de aprovisionamiento fino en el nivel del disco, se pueden crear discos virtuales en un formato fino. En un disco virtual fino, ESXi aprovisiona el espacio completo necesario para las actividades actuales y futuras del disco, por ejemplo, 40 GB. Sin embargo, el disco fino utiliza solo la cantidad de espacio que necesita el disco para las operaciones iniciales. En este ejemplo, el disco de aprovisionamiento fino ocupa solo 20 GB de almacenamiento. Si el disco requiere más espacio, puede expandirse hasta el total de 40 GB aprovisionados.



Acerca de las directivas de aprovisionamiento de discos virtuales

Cuando realiza ciertas operaciones de administración de máquina virtual, puede especificar una directiva de aprovisionamiento para el archivo de disco virtual. Las operaciones incluyen crear un disco virtual, clonar una máquina virtual a una plantilla o migrar una máquina virtual.

Los almacenes de datos NFS con aceleración de hardware y los almacenes de datos de VMFS admiten las siguientes directivas de aprovisionamiento de discos. En los almacenes de datos NFS que se no admite la aceleración de hardware, solo está disponible el formato fino.

Puede utilizar Storage vMotion o bien Storage vMotion entre hosts para pasar los discos virtuales de un formato a otro.

Puesta a cero lenta con aprovisionamiento grueso

Crea un disco virtual en un formato grueso predeterminado. El espacio necesario para el disco virtual se asigna en el momento en que se crea el disco. Los datos que quedan en el dispositivo físico no se borran durante la creación, sino que se ponen a cero según demanda más adelante, en la primera escritura de la máquina virtual. Las máquinas virtuales no leen datos obsoletos del dispositivo físico.

Puesta a cero rápida con aprovisionamiento grueso

Un tipo de disco virtual grueso que admite características de clúster, como Fault Tolerance. El espacio necesario para el disco virtual se asigna en el momento de la creación. A diferencia del formato de puesta a cero lenta de aprovisionamiento grueso, los datos que quedan en el dispositivo físico se ponen a cero cuando se crea el disco virtual. Es posible que la creación de discos virtuales en este formato demore más que la creación de otros tipos de disco. Aumentar el tamaño de un disco virtual grueso de puesta a cero rápida provoca un considerable tiempo de inactividad para la máquina virtual.

Aprovisionamiento fino

Utilice este formato para ahorrar espacio de almacenamiento. Para el disco fino, aprovisione tanto espacio de almacén de datos como lo requiera el disco, en función del valor que introduzca para el tamaño del disco virtual. Sin embargo, el disco fino comienza siendo pequeño y, al principio, utiliza solo el espacio de almacén de datos que necesita para las operaciones iniciales. Si posteriormente el disco fino necesita más espacio, puede aumentar su tamaño hasta la capacidad máxima y ocupar todo el espacio del almacén de datos aprovisionado para él.

El aprovisionamiento fino es el método más rápido para crear un disco virtual, ya que crea un disco solo con la información del encabezado. No asigna ni pone a cero los bloques de almacenamiento. Los bloques de almacenamiento se asignan y se ponen a cero la primera vez que se accede a ellos.

Nota Si un disco virtual admite soluciones de agrupación en clústeres, como Fault Tolerance, ese disco no debe tener aprovisionamiento fino.

Crear discos virtuales con aprovisionamiento fino

Para ahorrar espacio de almacenamiento, se puede crear un disco virtual en un formato de aprovisionamiento fino. El disco virtual con aprovisionamiento fino que se crea es pequeño y se expande a medida que se requiere más espacio en disco. Es posible crear discos finos únicamente en almacenes de datos compatibles con aprovisionamiento fino en el nivel de disco.

Este procedimiento da por sentado que se está creando una máquina virtual nueva. Para obtener información, consulte el documento *Administrar máquinas virtuales de vSphere*.

Procedimiento

1 Cree una máquina virtual.

   a Haga clic con el botón derecho en cualquier objeto de inventario que sea un objeto principal válido de una máquina virtual, como un centro de datos, una carpeta, un clúster, un grupo de recursos o un host, y seleccione **Nueva máquina virtual**.

   b Seleccione **Crear una nueva máquina virtual** y haga clic en **Siguiente**.

   c Siga los pasos necesarios para crear una máquina virtual.

2 Configure el disco virtual fino.

   a En la página Personalizar hardware, haga clic en la pestaña **Hardware virtual**.

   b Haga clic en el triángulo **Disco duro nuevo** para expandir las opciones del disco duro.

   c (opcional) Ajuste el tamaño de disco predeterminado.

   Con un disco virtual fino, el valor de tamaño de disco muestra cuánto espacio está aprovisionado y garantizado para el disco. Al principio, el disco virtual no puede utilizar todo el espacio aprovisionado. El valor de uso del almacenamiento real puede ser menor que el tamaño del disco virtual.

   d En Aprovisionamiento de disco, seleccione **Aprovisionamiento fino**.

3 Finalice la creación de la máquina virtual.

Resultados

Ha creado una máquina virtual con un disco en formato fino.

Pasos siguientes

Si se creó un disco virtual en el formato fino, más tarde se podrá expandir hasta su tamaño completo.

Ver los recursos de almacenamiento de una máquina virtual

Es posible ver cómo el espacio de almacenamiento del almacén de datos se asigna a las máquinas virtuales.

Procedimiento

1 Desplácese hasta la máquina virtual.

2 Haga doble clic en la máquina virtual y haga clic en la pestaña **Resumen**.

3 Puede revisar la información de uso del almacenamiento en el área superior derecha de la pestaña **Resumen**.

Resultados

En **Uso de almacenamiento**, se muestra cuánto espacio del almacén de datos ocupan los archivos de máquina virtual, incluidos los archivos de registro y configuración, las instantáneas, los discos

virtuales, etc. Cuando la máquina virtual está en ejecución, el espacio de almacenamiento utilizado también incluye archivos de intercambio.

En las máquinas virtuales con discos finos, el valor de uso de almacenamiento real puede ser inferior al tamaño del disco virtual.

Determinar el formato de disco de una máquina virtual

Puede determinar si el disco virtual tendrá formato grueso o fino.

Procedimiento

1 Haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.

2 Haga clic en la pestaña **Hardware virtual**.

3 Haga clic en el triángulo **Disco duro** para expandir las opciones de disco duro.

   El cuadro de texto **Tipo** muestra el formato del disco virtual.

Pasos siguientes

Si el disco virtual tiene formato fino, puede expandirlo a su tamaño completo.

Expandir discos virtuales finos

Si creó un disco virtual en formato fino, puede cambiarlo a un formato grueso.

Puede utilizar el explorador de almacenes de datos para expandir el disco virtual fino.

Requisitos previos

- Asegúrese de que el almacén de datos donde se encuentra la máquina virtual tenga espacio suficiente.
- Asegúrese de que el disco virtual sea fino.
- Quite las instantáneas.
- Apague la máquina virtual.

Procedimiento

1 En vSphere Client, desplácese hasta la carpeta del disco virtual que desea expandir.

   a Desplácese hasta la máquina virtual.

   b Haga clic en la pestaña **Almacenes de datos**.

      Se enumera el almacén de datos que almacena los archivos de la máquina virtual.

   c Haga clic con el botón derecho en el almacén de datos y seleccione **Examinar archivos**.

      El explorador del almacén de datos muestra el contenido del almacén de datos.

2 Expanda la carpeta de la máquina virtual y desplácese hasta el archivo del disco virtual que desea convertir.

   El archivo tiene la extensión `.vmdk` y está marcado con el icono de disco virtual ().

3 Seleccione el archivo de disco virtual y haga clic en **Expandir**.

   Nota Es posible que la opción no esté disponible si el disco virtual es grueso o si la máquina virtual está en ejecución.

Resultados

El disco virtual inflado ocupa el espacio del almacén de datos completo que se le aprovisionó originalmente.

Manejar la sobresuscripción del almacén de datos

Debido a que el espacio aprovisionado para los discos finos puede ser mayor que el espacio establecido, puede producirse una sobresuscripción del almacén de datos. En consecuencia, el espacio aprovisionado total para los discos de máquinas virtuales en el almacén de datos es mayor que la capacidad real.

La sobresuscripción puede ocurrir debido a que, por lo general, no todas las máquinas virtuales con discos finos necesitan simultáneamente todo el espacio del almacén de datos aprovisionado. Sin embargo, si desea evitar una sobresuscripción del almacén de datos, puede configurar una alarma que notifique el momento en el que espacio aprovisionado llega a un determinado umbral.

Para obtener información sobre la configuración de alarmas, consulte la documentación de *Administrar vCenter Server y hosts*.

Si las máquinas virtuales requieren más espacio, el espacio del almacén de datos se asigna por orden de llegada. Cuando el almacén de datos se queda sin espacio, puede agregar más almacenamiento físico y aumentar el almacén de datos.

Consulte Aumentar la capacidad de un almacén de datos de VMFS.

ESXi y aprovisionamiento fino de matrices

Puede utilizar matrices de almacenamiento de aprovisionamiento fino con ESXi.

El host ESXi se integra con el almacenamiento basado en bloques y realiza las siguientes tareas:

- El host puede reconocer LUN de aprovisionamiento fino subyacentes y supervisar su uso de espacio a fin de evitar quedarse sin espacio físico. El espacio del LUN puede cambiar si, por ejemplo, se expande el almacén de datos de VMFS o si se utiliza Storage vMotion para migrar máquinas virtuales al LUN de aprovisionamiento fino. El host le advierte sobre las vulneraciones del espacio físico del LUN y las condiciones de falta de espacio.

- El host puede ejecutar el comando `unmap` T10 automático desde los sistemas operativos invitados de VMFS6 y máquina virtual para recuperar el espacio sin utilizar de la matriz. VMFS5 admite un método de recuperación de espacio manual.

Nota ESXi no admite la habilitación y deshabilitación de aprovisionamiento fino en un dispositivo de almacenamiento.

Requisitos

Para usar los informes de aprovisionamiento fino y las funciones de recuperación de espacio, siga estos requisitos:

- Use una versión apropiada de ESXi.

Tabla 25-1. Versiones de ESXi y compatibilidad con aprovisionamiento fino

Componentes de aprovisionamiento fino compatibles	ESXi 6.0 y versiones anteriores	ESXi 6.5 y versiones posteriores
Aprovisionamiento fino	Sí	Sí
Comando Unmap de cancelación de asignación que se origina en VMFS	Manual para VMFS5. Use `esxcli storage vmfs unmap`.	Automático para VMFS6
Comando Unmap de cancelación de asignación que se origina en el sistema operativo invitado	Sí. Compatibilidad limitada.	Sí (VMFS6)

- Use sistemas de almacenamiento que admitan instancias de vSphere Storage APIs - Array Integration (VAAI) basadas en T10, que incluyan el aprovisionamiento fino y la recuperación de espacio. Para obtener información, póngase en contacto con el proveedor de almacenamiento y consulte la *Guía de compatibilidad de VMware*.

Supervisión del uso del espacio

La funcionalidad de integración de aprovisionamiento fino ayuda a supervisar el uso del espacio en los LUN con aprovisionamiento fino y a evitar quedarse sin espacio.

El flujo de muestra siguiente demuestra cómo el host ESXi y la matriz de almacenamiento interactúan para generar advertencias por infracción del espacio y falta de espacio en un LUN con aprovisionamiento fino. Se aplica el mismo mecanismo cuando se utiliza Storage vMotion para migrar máquinas virtuales al LUN con aprovisionamiento fino.

1. Mediante herramientas específicas de almacenamiento, el administrador de almacenamiento aprovisiona un LUN fino y establece un límite de umbral flexible que, cuando se alcanza, activa una alerta. Este paso es específico del proveedor.
2. Con vSphere Client, puede crear un almacén de datos de VMFS en el LUN con aprovisionamiento fino. El almacén de datos abarca el tamaño lógico completo que informa el LUN.

3 A medida que el espacio que utiliza el almacén de datos aumenta y se alcanza el umbral flexible establecido, se realizan las acciones siguientes:

   a La matriz de almacenamiento informa la infracción al host.

   b El host activa una alarma de advertencia para el almacén de datos.

   Puede ponerse en contacto con el administrador de almacenamiento para solicitar más espacio físico. Si lo prefiere, puede utilizar Storage vMotion para evacuar las máquinas virtuales antes de que el LUN se quede sin capacidad.

4 Si no queda espacio para asignar al LUN con aprovisionamiento fino, se realizan las acciones siguientes:

   a La matriz de almacenamiento informa la condición de falta de espacio al host.

   Precaución En ciertos casos, cuando un LUN se llena, puede desconectarse o desasignarse del host.

   b El host pausa las máquinas virtuales y genera una alarma por falta de espacio.

   Para solucionar la condición de falta de espacio permanente, solicite más espacio físico al administrador de almacenamiento.

Identificar dispositivos de almacenamiento de aprovisionamiento fino

Use el comando `esxcli` para comprobar si un dispositivo de almacenamiento particular es de aprovisionamiento fino.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

- Ejecute el comando **esxcli storage core device list -d=*device_ID***.

Resultados

El estado de aprovisionamiento fino siguiente indica que el dispositivo de almacenamiento es de aprovisionamiento fino.

```
# esxcli storage core device list -d naa.XXXXXXXXXXXX4c
naa.XXXXXXXXXXXX4c
 Display Name: XXXX Fibre Channel Disk(naa.XXXXXXXXXXXX4c)
 Size: 20480
 Device Type: Direct-Access
 Multipath Plugin: NMP
 ---------------------
 Thin Provisioning Status: yes
 ---------------------
```

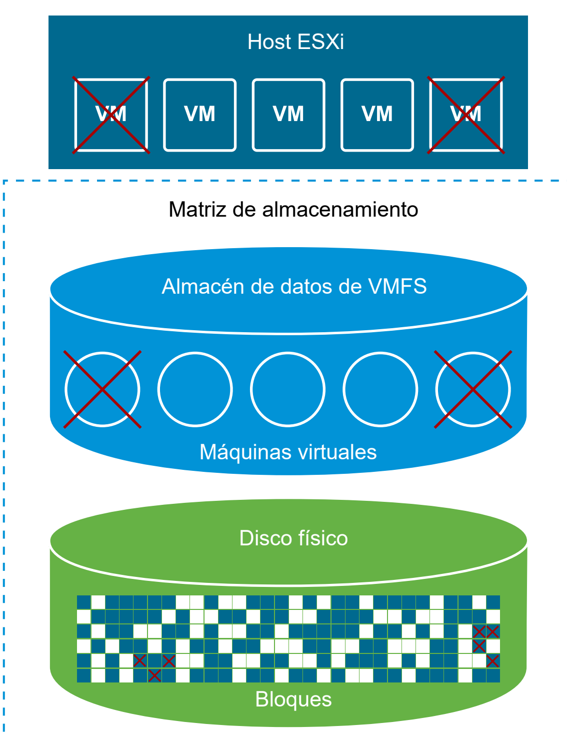
Un estado desconocido indica que el dispositivo de almacenamiento es grueso.

Nota Algunos sistemas de almacenamiento presentan todos los dispositivos como de aprovisionamiento fino, sin importar si los dispositivos son finos o gruesos. El estado de aprovisionamiento fino siempre es `yes`. Para obtener más información, consulte al proveedor de almacenamiento.

Recuperación de espacio de almacenamiento

ESXi admite el comando de recuperación de espacio, también denominado comando unmap de cancelación de asignación de SCSI, que se origina en un almacén de datos de VMFS o un sistema operativo invitado de máquina virtual. El comando ayuda a que las matrices de almacenamiento con aprovisionamiento fino recuperen el espacio no utilizado del almacén de datos de VMFS y los discos virtuales del almacén de datos. El almacén de datos VMFS6 puede enviar el comando de recuperación de espacio automáticamente. Con el almacén de datos VMFS5, se puede recuperar manualmente el espacio de almacenamiento.

Se libera espacio de almacenamiento dentro del almacén de datos de VMFS al eliminar o migrar la máquina virtual o al consolidar una instantánea, entre otras acciones. Dentro de la máquina virtual, se libera espacio de almacenamiento cuando se eliminan archivos del disco virtual fino. Estas operaciones dejan bloques de espacio sin utilizar en la matriz de almacenamiento. Sin embargo, si la matriz no recibe información sobre la eliminación de datos de los bloques, sigue asignando los bloques hasta que el almacén de datos los libera. VMFS utiliza el comando unmap de cancelación de asignación de SCSI para indicar a la matriz que los bloques de almacenamiento contienen datos eliminados, de modo que la matriz pueda cancelar la asignación de estos bloques.



El comando también puede originarse directamente en el sistema operativo invitado. Tanto los almacenes de datos de VMFS5 como los de VMFS6 pueden admitir el comando unmap de cancelación de asignación proveniente del sistema operativo invitado. Sin embargo, el grado de compatibilidad en VMFS5 es limitado.

Según el tipo de almacén de datos de VMFS, puede utilizar diferentes métodos para configurar la recuperación de espacio para el almacén de datos y las máquinas virtuales.

Vea el siguiente vídeo para obtener más información sobre el funcionamiento de la recuperación de espacio.

(Recuperación de espacio con VMFS)

- Solicitudes de recuperación de espacio de almacenes de datos de VMFS

  Al eliminar o quitar archivos de un almacén de datos de VMFS, se libera espacio en el sistema de archivos. Este espacio libre queda asignado a un dispositivo de almacenamiento hasta que el sistema de archivos lo libera o cancela la asignación. ESXi admite la recuperación de espacio libre, también denominada operación de cancelación de asignación.

- Solicitudes de recuperación de espacio de sistemas operativos invitados

  ESXi admite los comandos unmap de cancelación de asignación emitidos directamente desde un sistema operativo invitado para recuperar espacio de almacenamiento. El nivel de compatibilidad y los requisitos dependen del tipo de almacén de datos en el cual reside la máquina virtual.

Solicitudes de recuperación de espacio de almacenes de datos de VMFS

Al eliminar o quitar archivos de un almacén de datos de VMFS, se libera espacio en el sistema de archivos. Este espacio libre queda asignado a un dispositivo de almacenamiento hasta que el sistema de archivos lo libera o cancela la asignación. ESXi admite la recuperación de espacio libre, también denominada operación de cancelación de asignación.

La operación ayuda a que la matriz de almacenamiento recupere espacio libre sin utilizar. El espacio sin asignar puede volver a utilizarse para otras necesidades y solicitudes de asignación de almacenamiento.

Recuperación asíncrona de espacio libre en un almacén de datos de VMFS6

En los almacenes de datos de VMFS6, ESXi admite la recuperación asíncrona automática de espacio libre. VMFS6 puede ejecutar el comando unmap para liberar espacio de almacenamiento libre en segundo plano en las matrices de almacenamiento con aprovisionamiento fino compatibles con estas operaciones de cancelación de asignación.

El procesamiento asíncrono de cancelaciones de asignación tiene varias ventajas:

- Las solicitudes de cancelación de asignación se envían a un ritmo constante, lo cual ayuda a evitar la carga repentina de la matriz.

- Las regiones liberadas se agrupan y su asignación se cancela simultáneamente.
- El comando unmap no afecta al rendimiento de E/S de otras cargas de trabajo.

Para almacenes de datos de VMFS6, puede configurar los siguientes parámetros de recuperación de espacio.

Granularidad de la recuperación de espacio

La granularidad define el tamaño mínimo del sector de espacio liberado que puede recuperar el almacenamiento subyacente. El almacenamiento no puede recuperar los sectores de tamaño menor a la granularidad especificada.

Para VMFS6, la granularidad de recuperación es equivalente al tamaño del bloque. Cuando se especifica un tamaño de bloque de 1 MB, la granularidad también es de 1 MB. Los sectores de almacenamiento con un tamaño inferior a 1 MB no se recuperan.

Nota En algunas matrices de almacenamiento, se recomienda una granularidad óptima para la cancelación de asignación. ESXi admite el procesamiento de cancelaciones de asignación automáticas en matrices con la granularidad de cancelación recomendada de 1 MB o superior, por ejemplo, 16 MB. En las matrices con la granularidad óptima de hasta 1 MB, la operación de cancelación de asignación se admite si la granularidad es un factor de 1 MB. Por ejemplo, 1 MB es divisible por 512 bytes, 4 KB, 64 KB, etc.

Método de recuperación de espacio

El método puede ser recuperación de prioridad o fija. Cuando el método de recuperación es la prioridad, se configura la tasa de prioridad. Para el método fijo, debe indicar el ancho de banda en MB por segundo.

Prioridad de recuperación de espacio

Este parámetro define la tasa a la que se realiza la operación de recuperación de espacio cuando se utiliza el método de recuperación de prioridad. Generalmente, VMFS6 puede enviar los comandos unmap de cancelación de asignación en ráfagas o esporádicamente, según la carga de trabajo y la configuración. Para VMFS6, puede especificar una de las siguientes opciones.

Prioridad de recuperación de espacio	Descripción	Configuración
Ninguna	Deshabilita las operaciones de cancelación de asignación para el almacén de datos.	vSphere Client comando `esxcli`
Baja (predeterminado)	Envía el comando de cancelación de asignación con menor frecuencia, de 25 a 50 MB por segundo.	vSphere Client comando `esxcli`

Prioridad de recuperación de espacio	Descripción	Configuración
Mediano	Envía el comando a una velocidad dos veces más rápida que la velocidad baja, de 50 a 100 MB por segundo.	comando `esxcli`
Alto	Envía el comando a una velocidad tres veces más rápida que la velocidad baja, más de 100 MB por segundo.	comando `esxcli`

Nota El host ESXi de la versión 6.5 no reconoce las tasas de prioridad media y alta. Si se migran las máquinas virtuales a la versión de host 6.5, la tasa es baja de forma predeterminada.

Después de habilitar la recuperación de espacio, el almacén de datos de VMFS6 podrá comenzar a liberar los bloques de espacio sin utilizar únicamente cuando tenga al menos un archivo abierto. Esta condición puede cumplirse cuando, por ejemplo, se enciende una de las máquinas virtuales en el almacén de datos.

Recuperación manual de espacio libre en un almacén de datos de VMFS5

VMFS5 y los sistemas de archivos anteriores no cancelan la asignación del espacio libre automáticamente, pero se puede utilizar el comando `esxcli storage vmfs unmap` para recuperar espacio de forma manual. Cuando utilice el comando, tenga en cuenta que puede enviar varias solicitudes de cancelación de asignación a la vez. Esta acción puede bloquear algunos de los recursos durante la operación.

Configurar la recuperación de espacio para un almacén de datos de VMFS6

Cuando se crea un almacén de datos de VMFS6, se pueden modificar los parámetros predeterminados para la recuperación de espacio automática.

En el momento de la creación del almacén de datos de VMFS6, el único método disponible para la recuperación de espacio es la prioridad. Para utilizar el método fijo, edite la configuración de recuperación de espacio del almacén de datos existente.

Procedimiento

1 En el navegador de objetos de vSphere Client, vaya hasta un host, un clúster o un centro de datos.

2 En el menú contextual, seleccione **Almacenamiento > Nuevo almacén de datos**.

3 Siga los pasos necesarios para crear un almacén de datos de VMFS6.

4 En la página **Configuración de particiones**, especifique los parámetros de recuperación de espacio.

Los parámetros definen la granularidad y el índice de prioridad con que se realizan las operaciones de recuperación de espacio. También puede usar esta página para deshabilitar la recuperación de espacio para el almacén de datos.

Opción	Descripción
Tamaño de bloque	El tamaño de bloque de un almacén de datos de VMFS define el tamaño de archivo máximo y la cantidad de espacio que ocupa el archivo. VMFS6 admite el tamaño de bloque de 1 MB.
Granularidad de la recuperación de espacio	Especifique la granularidad de la operación de cancelación de la asignación. La granularidad de cancelación de la asignación equivale al tamaño de bloque, que es de 1 MB. Los sectores de almacenamiento con un tamaño menor a 1 MB no se recuperan.
Prioridad de recuperación de espacio	Seleccione una de las siguientes opciones. ■ Baja (predeterminado). Utilice el método de prioridad para la recuperación de espacio. Habilite la operación de cancelación de asignación a un índice de prioridad bajo. ■ Ninguna. Seleccione esta opción si quiere deshabilitar las operaciones de recuperación de espacio para el almacén de datos.

Nota En vSphere Client, la única configuración disponible para la prioridad de recuperación de espacio es Baja y Ninguna. Para cambiar la configuración a Media o Alta, utilice el comando `esxcli`. Consulte Utilizar el comando ESXCLI para cambiar los parámetros de recuperación de espacio.

5 Finalice el proceso de creación del almacén de datos.

Resultados

Después de habilitar la recuperación de espacio, el almacén de datos de VMFS6 podrá comenzar a liberar los bloques de espacio sin utilizar únicamente cuando tenga al menos un archivo abierto. Esta condición puede cumplirse cuando, por ejemplo, se enciende una de las máquinas virtuales en el almacén de datos.

Cambiar la configuración de recuperación de espacio

Al crear un almacén de datos de VMFS6 en vSphere Client, el único método para recuperar espacio que puede especificarse es el método de prioridad. Para habilitar el método fijo, modifique la configuración de recuperación espacio en el almacén de datos actual.

Procedimiento

1 En vSphere Client, desplácese al almacén de datos.

2 Seleccione **Editar recuperación de espacio** en el menú contextual.

3 Especifique la configuración de recuperación de espacio.

Opción	Descripción
Habilitar recuperación de espacio automática con tasa fija	Utilice el método fijo para la recuperación de espacio. Especifique el ancho de banda de recuperación en MB por segundo.
Deshabilitar recuperación de espacio automática	Los bloques eliminados o sin asignar no se recuperan.

4 Haga clic en **Aceptar** para guardar la nueva configuración.

5 Desmonte y vuelva a montar el almacén de datos para que se apliquen los cambios.

   a Desmontar almacenes de datos.

   b Montar almacenes de datos.

6 Repita este procedimiento en todos los hosts ESXi que accedan al almacén de datos.

Resultados

El valor modificado para la prioridad de recuperación de espacio aparece en la página **General** correspondiente al almacén de datos.

Utilizar el comando ESXCLI para cambiar los parámetros de recuperación de espacio

Puede cambiar la prioridad de recuperación de espacio, la granularidad y otros parámetros predeterminados.

Procedimiento

1 En el host ESXi, use el siguiente comando para establecer los parámetros de recuperación de espacio.

```
esxcli storage vmfs reclaim config set
```

Este comando toma estas opciones:

Opción	Descripción
-b|--reclaim-bandwidth	Ancho de banda fijo de recuperación de espacio en MB por segundo.
-g|--reclaim-granularity	Granularidad mínima de recuperación de espacio automática en bytes.
-m|--reclaim-method	Método de recuperación de espacio automática. Opciones admitidas: ■ prioridad ■ fija
-p|--reclaim-priority	Prioridad de la recuperación de espacio automática. Opciones admitidas: ■ none ■ baja ■ mediana ■ alta

Opción	Descripción
-l|--volume-label	La etiqueta del volumen VMFS de destino.
-u|--volume-uuid	El UUID del volumen VMFS de destino.

Puede utilizar los siguientes ejemplos.

- Establezca el método de recuperación como fijo y la velocidad como 100 MB por segundo.

```
esxcli storage vmfs reclaim config set --volume-label datastore_name --reclaim-method
fixed -b 100
```

- Desactive la recuperación de espacio automática de VMFS.

```
esxcli storage vmfs reclaim config set --volume-label datastore_name --reclaim-
priority none
```

2 Desmonte el almacén de datos de VMFS6 de todos los demás hosts ESXi donde está montado el almacén de datos y vuelva a montarlo.

a Desmontar almacenes de datos.

b Montar almacenes de datos.

Este paso garantiza que todos los hosts ESXi en los que se montó el almacén de datos de VMFS6 cambien al método de recuperación fijo del almacén de datos.

Comprobar la configuración de la recuperación de espacio automática

Después de configurar o editar los parámetros de recuperación de espacio para un almacén de datos de VMFS6, puede revisar la configuración.

Procedimiento

1 En vSphere Client, desplácese al almacén de datos.

2 Haga clic en la pestaña **Configurar**.

3 Haga clic en **General** y compruebe la configuración de recuperación de espacio.

a En Propiedades, expanda **Sistema de archivos** y revise el valor de granularidad de la recuperación de espacio.

b En Recuperación de espacio, revise la configuración de prioridad de la recuperación de espacio.

Si configuró algún valor mediante el comando `esxcli`, por ejemplo, una prioridad Media o Alta de recuperación de espacio, estos valores también aparecen en vSphere Client.

Ejemplo: Obtención de parámetros para la recuperación de espacio de VMFS6

También puede utilizar el comando **esxcli storage vmfs reclaim config get -l=*VMFS_label*|-u=*VMFS_uuid*** para obtener información sobre la configuración de recuperación de espacio.

```
# esxcli storage vmfs reclaim config get -l my_datastore
Reclaim Granularity: 1048576 Bytes
Reclaim Priority: low
```

Recuperar manualmente espacio de almacenamiento acumulado

En los almacenes de datos VMFS que no admiten la recuperación de espacio automática, puede utilizar el comando `esxcli` para recuperar manualmente el espacio de almacenamiento no utilizado.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 Para recuperar bloques de almacenamiento no utilizados en el dispositivo con aprovisionamiento fino, ejecute el siguiente comando:

  esxcli storage vmfs unmap

  Este comando toma estas opciones:

Opción	Descripción
-l|--volume-label=*volume_label*	La etiqueta del volumen VMFS cuya asignación se desea anular. Un argumento obligatorio. Si especifica este argumento, no utilice **-u|--volume-uuid=*volume_uuid***.
-u|--volume-uuid=*volume_uuid*	El UUID del volumen VMFS cuya asignación se desea anular. Un argumento obligatorio. Si especifica este argumento, no utilice **-l|--volume-label=*volume_label***.
-n|--reclaim-unit=*number*	Cantidad de bloques VMFS cuya asignación se desea anular por iteración. Un argumento opcional. Si no se especifica, el comando utiliza el valor predeterminado de 200.

2 Para comprobar si finalizó el proceso de cancelación de asignación, busque la cancelación de asignación en el archivo `vmkernel.log`.

Solicitudes de recuperación de espacio de sistemas operativos invitados

ESXi admite los comandos unmap de cancelación de asignación emitidos directamente desde un sistema operativo invitado para recuperar espacio de almacenamiento. El nivel de compatibilidad y los requisitos dependen del tipo de almacén de datos en el cual reside la máquina virtual.

Dentro de una máquina virtual, se libera espacio de almacenamiento cuando, por ejemplo, se eliminan archivos del disco virtual fino. El sistema operativo invitado notifica a VMFS sobre la liberación de espacio mediante el comando unmap de cancelación de asignación. El comando unmap de cancelación de asignación enviado desde el sistema operativo invitado libera espacio dentro del almacén de datos de VMFS. Luego, el comando se transmite a la matriz para que esta pueda recuperar los bloques de espacio liberados.

Recuperación de espacio para máquinas virtuales VMFS6

VMFS6 generalmente admite las solicitudes de recuperación automática de espacio que se generan en los sistemas operativos invitados y las transmite a la matriz. Muchos sistemas operativos invitados pueden enviar un comando unmap de cancelación de asignación sin necesidad de configuración adicional. En el caso de los sistemas operativos invitados que no admiten comandos unmap automáticos, puede ser necesaria la intervención del usuario. Para obtener información sobre los sistemas operativos invitados que admiten la recuperación de espacio automática en VMFS6, póngase en contacto con el proveedor.

Generalmente, los sistemas operativos invitados envían los comandos unmap de cancelación de asignación de acuerdo con la granularidad de cancelación de asignación que informan. Puede encontrar más detalles al respecto en la documentación suministrada con el sistema operativo invitado.

Cuando se usa la recuperación de espacio con VMFS6, se aplican las consideraciones siguientes:

- VMFS6 procesa la solicitud de cancelación de asignación del SO invitado únicamente cuando el espacio que se desea recuperar equivale a 1 MB o es un múltiplo de 1 MB. Si el espacio es menor que 1 MB o no está alineado con 1 MB, no se procesan las solicitudes de cancelación de asignación.
- Para las máquinas virtuales con instantáneas en el formato predeterminado de SEsparse, VMFS6 admite la recuperación de espacio automática solo en los hosts ESXi 6.7 o de una versión posterior.

  La recuperación de espacio afecta solo a la primera instantánea y funciona cuando la máquina virtual está encendida.

Recuperación de espacio para máquinas virtuales VMFS5

Generalmente, el comando unmap de cancelación de asignación generado en el sistema operativo invitado en VMFS5 no puede transmitirse directamente a la matriz. Es necesario ejecutar el comando `esxcli storage vmfs unmap` para activar la cancelación de asignaciones en la matriz.

Sin embargo, para unos pocos sistemas operativos invitados, VMFS5 admite las solicitudes de recuperación de espacio automática.

Para enviar las solicitudes de cancelación de asignación del sistema operativo invitado a la matriz, la máquina virtual debe cumplir los siguientes requisitos previos:

- El disco virtual debe tener aprovisionamiento fino.

- El hardware de la máquina virtual debe corresponder a la versión 11 (ESXi 6.0) o una versión posterior.
- El parámetro de configuración avanzada EnableBlockDelete debe estar configurado en 1.
- El sistema operativo invitado debe ser capaz de identificar el disco virtual como fino.

Introducción a Almacenamiento nativo en la nube 26

Almacenamiento nativo en la nube es una solución que proporciona una administración de datos integral de las aplicaciones con estado. Cuando se utiliza Almacenamiento nativo en la nube, se pueden crear las aplicaciones con estado en contenedor capaces de resistir reinicios e interrupciones. Los contenedores con estado aprovechan el almacenamiento que vSphere expone mientras usan primitivos como volúmenes estándar, volúmenes persistentes o aprovisionamiento dinámico.

Mediante Almacenamiento nativo en la nube, se pueden crear volúmenes contenedores persistentes que sean independientes del ciclo de vida del contenedor y la máquina virtual. El almacenamiento de vSphere respalda los volúmenes; asimismo, se puede establecer una directiva de almacenamiento directamente en los volúmenes. Después de crear los volúmenes, puede revisar tanto estos como sus objetos de almacenamiento de respaldo en vSphere Client, así como supervisar el cumplimiento de la directiva de almacenamiento.

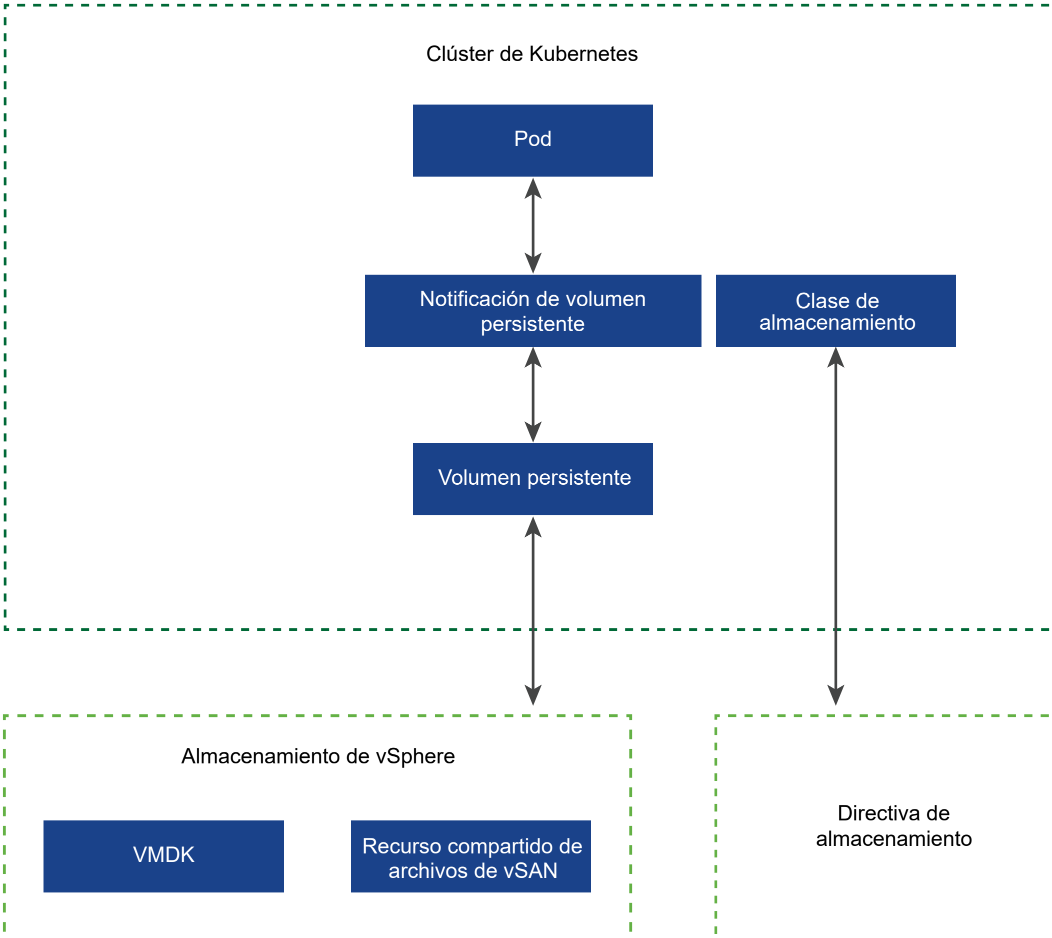
El Almacenamiento nativo en la nube de vSphere es compatible con volúmenes persistentes en las siguientes distribuciones de Kubernetes:

- Kubernetes genérico, también denominado virgen, que se instala desde los repositorios oficiales. Esta documentación de *Almacenamiento de vSphere* abarca solo Kubernetes genérico.
- vSphere with Tanzu. Para obtener más información, consulte la documentación sobre *Configuración y administración de vSphere with Tanzu*.

Este capítulo incluye los siguientes temas:

Conceptos y terminología del Almacenamiento nativo en la nube

Familiarícese con varios conceptos fundamentales para el entorno de Almacenamiento nativo en la nube de vSphere.



Clúster de Kubernetes

En el entorno de Almacenamiento nativo en la nube, puede implementar un clúster de Kubernetes genérico en un clúster de máquinas virtuales. Las aplicaciones en contenedor se implementan sobre el clúster de Kubernetes. Las aplicaciones pueden tener estado o no.

Nota Para obtener información sobre clústeres superiores y clústeres de TKG que se pueden ejecutar en vSphere with Tanzu, consulte la documentación de *Configuración y administración de vSphere with Tanzu*.

Pod

Un pod es un grupo de una o varias aplicaciones en contenedor que comparten recursos como el almacenamiento y la red. Los contenedores dentro de un pod se inician, se detienen y se replican como un grupo.

Orquestador de contenedores

Plataformas de código abierto (como Kubernetes) para implementar, escalar y administrar las aplicaciones en contenedor en clústeres de hosts. Las plataformas proporcionan una infraestructura centrada en contenedores.

Aplicación con estado

A medida que las aplicaciones en contenedor pasan de no tener estado a tenerlo, requieren un almacenamiento persistente. A diferencia de las aplicaciones sin estado, las cuales no guardan datos entre sesiones, las aplicaciones con estado sí guardan datos en un almacenamiento persistente. Estos datos que se conservan se denominan estado de la aplicación. Posteriormente, puede recuperarlos y utilizarlos en la siguiente sesión. La mayoría de las aplicaciones tienen estado. Una base de datos es un ejemplo de una aplicación con estado.

PersistentVolume

Las aplicaciones con estado utilizan objetos PersistentVolume para almacenar sus datos. Un objeto PersistentVolume es un volumen de Kubernetes capaz de conservar su estado y sus datos. Es independiente de un pod y puede seguir existiendo incluso cuando el pod se elimina o se vuelve a configurar. En el entorno de vSphere, los objetos de PersistentVolume usan discos virtuales de vSphere de tipo de disco de primera clase (First Class Disk, FCD) o recursos compartidos de archivos de vSAN como almacenamiento de respaldo. Los discos de primera clase también se denominan discos virtuales mejorados (Improved Virtual Disks, IVD) o discos virtuales administrados.

- Los discos virtuales admiten volúmenes montados como ReadWriteOnce. Un único pod puede usar estos volúmenes en Kubernetes.

  A partir de vSphere 7.0, puede utilizar la tecnología de cifrado de vSphere para proteger los discos virtuales de FCD que respaldan los volúmenes persistentes. Para obtener más información, consulte Usar cifrado con almacenamiento nativo en la nube.

- Los recursos compartidos de archivos de vSAN admiten volúmenes de ReadWriteMany montados por varios nodos. Estos volúmenes pueden compartirse entre varios pods o aplicaciones que se ejecutan en nodos de Kubernetes o en clústeres de Kubernetes. Para obtener información sobre las posibles configuraciones con recursos compartidos de archivos, consulte Usar servicio de archivos de vSAN para aprovisionar volúmenes de archivos.

StorageClass

Kubernetes utiliza una StorageClass para definir diferentes niveles de almacenamiento y para describir diferentes tipos de requisitos de almacenamiento que respaldan PersistentVolume. En el entorno de vSphere, una clase de almacenamiento se puede vincular con una directiva de almacenamiento. Como administrador de vSphere, cree directivas de almacenamiento que describan diferentes requisitos de almacenamiento. Las directivas de almacenamiento de máquina virtual pueden usarse como parte de la definición StorageClass del aprovisionamiento dinámico de volúmenes.

El siguiente archivo YAML de ejemplo hace referencia a la directiva de almacenamiento **`Gold`** que creó anteriormente con vSphere Client. El VMDK de volumen persistente resultante se ubica en un almacén de datos compatible que cumple con los requisitos de la directiva de almacenamiento **`Gold`**.

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: gold-sc
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: csi.vsphere.vmware.com
parameters:
  storagepolicyname: "Gold"
```

PersistentVolumeClaim

Generalmente, las aplicaciones o los pods pueden solicitar almacenamiento persistente a través de PersistentVolumeClaim. PersistentVolumeClaim especifica el tipo y la clase de almacenamiento, el modo de acceso, ya sea ReadWriteOnce o ReadWriteMany, y otros parámetros para PersistentVolume. A continuación, la solicitud puede aprovisionar de forma dinámica el objeto de PersistentVolume correspondiente y el disco virtual subyacente o el recurso compartido de archivos de vSAN en el entorno de vSphere.

Cuando se crea la reclamación, PersistentVolume se enlaza automáticamente a ella. Los pods usan la reclamación para montar el objeto PersistentVolume y acceder al almacenamiento.

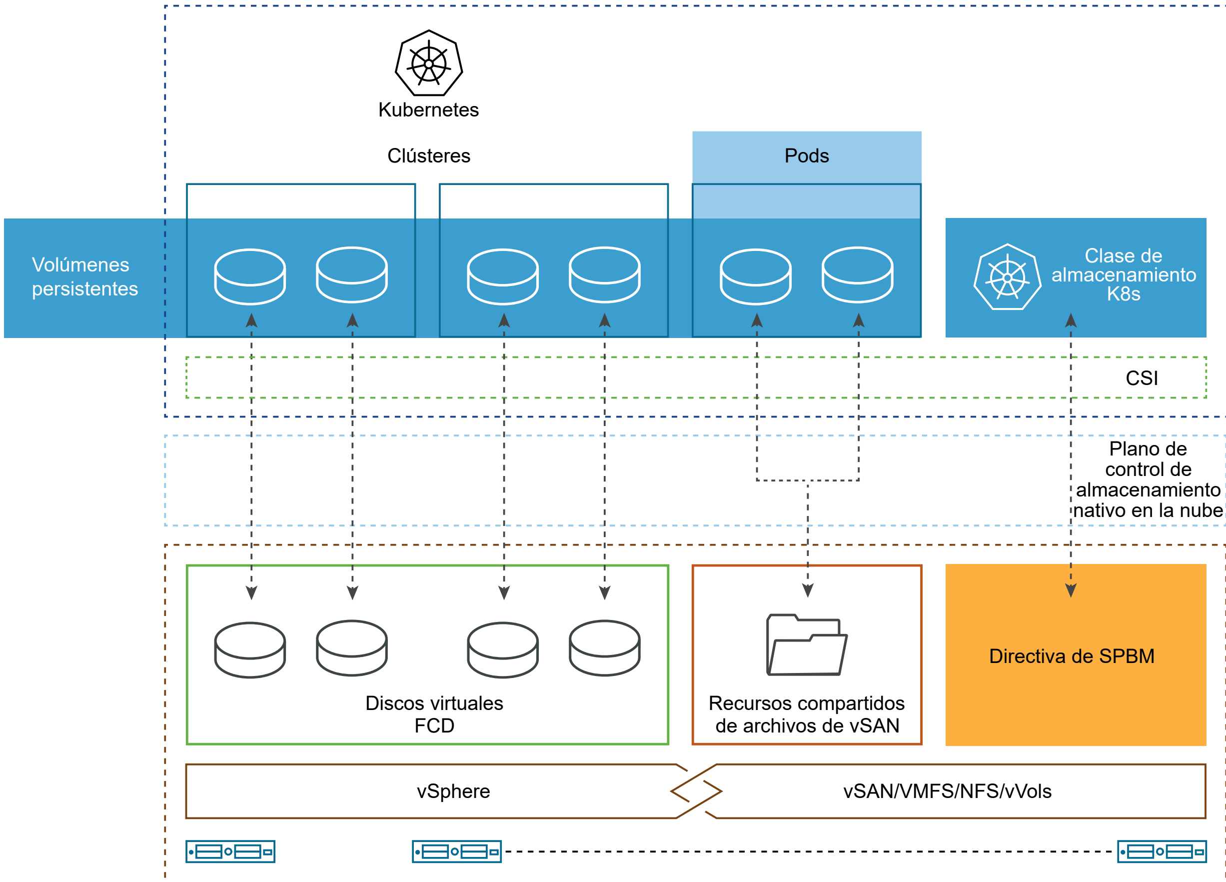
Cuando esta notificación se elimina, se eliminan también el objeto PersistentVolume y el almacenamiento subyacente.

```
kind: PersistentVolumeClaim
metadata:
 name: persistent-VMDK
spec:
 accessModes:
 - ReadWriteOnce
 resources:
 requests:
 storage: 5Gi
 storageClassName: gold-sc
```

Componentes de Almacenamiento nativo en la nube

Almacenamiento nativo en la nube utiliza varios componentes para integrarse con el almacenamiento de vSphere.

En la siguiente imagen se muestra cómo interactúan estos componentes.



Clúster de Kubernetes

En el entorno de Almacenamiento nativo en la nube, un clúster de Kubernetes genérico se implementa en un clúster de máquinas virtuales o nodos que se ejecutan en vSphere. Un usuario de Kubernetes interactúa directamente con el clúster cuando implementa aplicaciones con estado sobre él.

Nota Para obtener información sobre clústeres superiores y clústeres de TKG que se pueden ejecutar en vSphere with Tanzu, consulte la documentación de *Configuración y administración de vSphere with Tanzu*.

Interfaz de almacenamiento de contenedor (CSI) para vSphere

Para consumir los recursos de la infraestructura subyacente, el clúster requiere un controlador de CSI.

La interfaz de almacenamiento de contenedor (Container Storage Interface, CSI) de vSphere es un complemento fuera de la lista que expone el almacenamiento de vSphere a cargas de trabajo en orquestadores de contenedores, como Kubernetes. El complemento habilita vSAN y otros tipos de almacenamiento de vSphere.

CSI de vSphere se comunica con el plano de control de CNS en vCenter Server para todas las operaciones de aprovisionamiento de almacenamiento. La CSI de vSphere admite las siguientes funcionalidades:

- Aprovisionamiento dinámico de volúmenes de contenedor.
- La funcionalidad First Class Disk de vSphere.
- Zonas de Kubernetes.
- Montajes convencionales y sin formato.
- Una única instancia de vCenter Server y varios centros de datos y clústeres.
- Aprovisionamiento desde varios almacenes de datos o clústeres de almacenes de datos.
- Servicio de archivos de vSAN

En Kubernetes, el controlador de CSI se utiliza con la interfaz de proveedor de nube (CPI) de vSphere fuera de la lista. El controlador de CSI se envía como una imagen de contenedor, y el administrador de clústeres debe implementarlo. Para obtener más información, consulte la sección Implementación de controladores de la documentación sobre el controlador CSI de vSphere para Kubernetes en Github.

Para obtener información sobre las variaciones de CSI que se utilizan en los clústeres supervisores y los clústeres de TKG que se pueden ejecutar en vSphere with Tanzu, consulte la documentación de *Configuración y administración de vSphere with Tanzu*.

Componente de servidor de Almacenamiento nativo en la nube

El componente de servidor de CNS, o el plano de control de CNS, reside en vCenter Server. Se trata de una extensión de administración de vCenter Server que implementa las operaciones de aprovisionamiento y ciclo de vida de los volúmenes contenedores.

Cuando se aprovisionan volúmenes de contenedores, interactúa con vCenter Server para crear objetos de almacenamiento que respaldan dichos volúmenes. La funcionalidad de administración de almacenamiento basada en directivas garantiza el nivel de servicio que requieren los volúmenes.

El almacenamiento nativo en la nube también realiza operaciones de consulta que permiten administrar y supervisar volúmenes de contenedores y sus objetos de almacenamiento de respaldo a través de vCenter Server.

Disco de primera clase (First Class Disk, FCD)

También se denomina disco virtual mejorado (Improved Virtual Disk, IVD) o disco virtual administrado. Se trata de un disco virtual designado que no está asociado con ninguna máquina virtual. Estos discos residen en un almacén de datos de vSAN, VMFS, NFS o vVols, y brindan respaldo a los volúmenes de contenedores de ReadWriteOnce.

La tecnología FCD permite realizar operaciones de ciclo de vida relacionadas con volúmenes persistentes fuera del ciclo de vida de la máquina virtual o del pod. Si la máquina virtual es un nodo de Kubernetes que ejecuta varias aplicaciones basadas en contenedor y utiliza volúmenes persistentes y discos virtuales para muchas aplicaciones, CNS facilita las operaciones de ciclo de vida en el contenedor y la granularidad del volumen persistente.

Servicio de archivos de vSAN

Se trata de una capa de vSAN que proporciona recursos compartidos de archivos. Actualmente admite recursos compartidos de archivos NFSv3 y NFSv4.1. Almacenamiento nativo en la nube utiliza recursos compartidos de archivos de vSAN para volúmenes persistentes del tipo ReadWriteMany. Un único volumen ReadWriteMany se puede montar en varios nodos. El volumen se puede compartir entre varios pods o aplicaciones que se ejecuten en nodos de Kubernetes o en clústeres de Kubernetes.

Administración de almacenamiento basada en directivas

La administración de almacenamiento basada en directivas es un servicio de vCenter Server que admite el aprovisionamiento de volúmenes persistentes de acuerdo con los requisitos de almacenamiento especificados. Después del aprovisionamiento, el servicio supervisa el cumplimiento del volumen con las características de directiva requeridas.

Usar servicio de archivos de vSAN para aprovisionar volúmenes de archivos

El servicio de archivos de vSAN ofrece recursos compartidos de archivos de vSAN consumidos por volúmenes persistentes del tipo ReadWriteMany (RWM). Varios nodos pueden montar un solo volumen RWM. El volumen se puede compartir entre varios pods o aplicaciones que se ejecuten en nodos de Kubernetes o en clústeres de Kubernetes.

Cuando un pod de Kubernetes solicita un volumen RWM, Almacenamiento nativo en la nube se comunica con el servicio de archivos de vSAN para crear un recurso compartido de archivos basado en NFS de la clase de almacenamiento y tamaño solicitados. A continuación, Almacenamiento nativo en la nube monta el volumen RWM en el nodo de trabajo de Kubernetes en el que se ejecuta el pod. Si varios nodos solicitan acceso al volumen RWM, Almacenamiento nativo en la nube determina que el volumen RWM ya existe para esa implementación en particular y monta el volumen existente en los nodos.

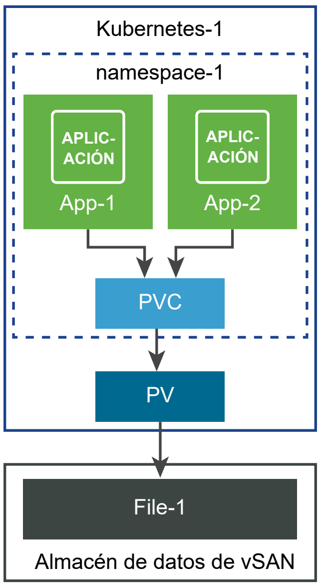
Para poder admitir volúmenes RWM, el entorno debe incluir los siguientes elementos.

- vSphere 7.0 y versiones posteriores con vSAN
- Servicio de archivos de vSAN habilitado. Para obtener información, consulte el documento *Administrar VMware vSAN*.
- Kubernetes 1.14 y versiones posteriores
- Versión compatible de CSI. Para obtener información, consulte la documentación del controlador de Kubernetes vSphere CSI en GitHub.

Puede utilizar diferentes configuraciones para los volúmenes de archivos.

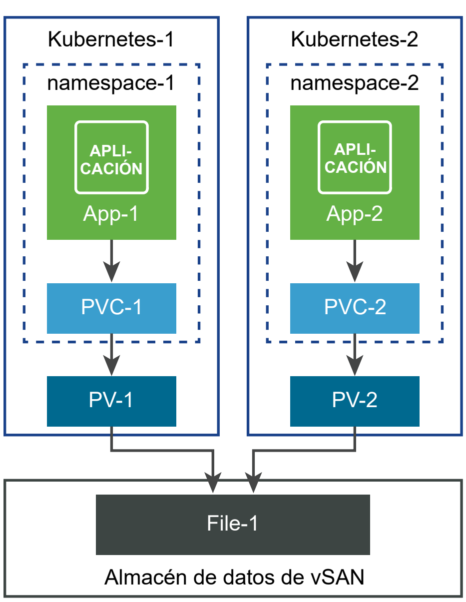
Volumen de archivos único compartido entre aplicaciones en el mismo espacio de nombres

En este ejemplo, se utiliza un solo volumen de archivos como almacenamiento compartido en diferentes aplicaciones en el mismo espacio de nombres. Puede utilizar una notificación de volumen persistente única para aprovisionar el volumen de archivos.



Volumen de archivos único compartido entre aplicaciones y espacios de nombres

En este ejemplo se utiliza un solo volumen de archivos como almacenamiento compartido en diferentes aplicaciones y espacios de nombres. Para cada espacio de nombres, se crea una notificación de volumen persistente independiente para aprovisionar el mismo volumen de archivos.



Usuarios de Almacenamiento nativo en la nube

Los tipos de usuarios que participan en el proceso de creación y supervisión de volúmenes de Kubernetes en el entorno de Almacenamiento nativo en la nube de vSphere se suelen dividir en dos categorías: usuario de Kubernetes y administrador de vSphere. Ambos tipos de usuarios tienen acceso a diferentes herramientas y realizan tareas distintas.

Usuario de Kubernetes de CNS

El usuario de Kubernetes puede ser un desarrollador de Kubernetes, un propietario de aplicaciones, un administrador de Kubernetes o una combinación de ambas funciones. Entre las tareas que realiza el usuario de Kubernetes en el entorno de Almacenamiento nativo en la nube se encuentran las siguientes:

- Implemente y administre vSphere CSI. Para obtener información, consulte la sección Implementación de vSphere Container Plug-in de la documentación Introducción a VMware vSphere Container Storage Plug-in.
- Aprovisione los volúmenes persistentes. Para obtener información acerca de los volúmenes de bloques, consulte Controlador CSI de vSphere: volumen de bloques. Para obtener información sobre los volúmenes de archivos, consulte Controlador CSI de vSphere: volumen de archivos.
- Realizar operaciones de ciclo de vida de volúmenes persistentes.
- Realizar operaciones de ciclo de vida de clases de almacenamiento.

Usuario de CNS de vSphere

Un usuario de CNS de vSphere o un administrador de vSphere tiene acceso a vSphere Client para realizar las siguientes tareas:

- Realizar operaciones de ciclo de vida de directivas de almacenamiento de máquina virtual. Por ejemplo, cree una directiva de almacenamiento de máquina virtual que se usará en una clase de almacenamiento de Kubernetes e indique su nombre al usuario de Kubernetes. Consulte Crear una directiva de almacenamiento para Kubernetes.
- Use la sección de Almacenamiento nativo en la nube de vSphere Client para supervisar el cumplimiento de las directivas de estado y de almacenamiento de los volúmenes contenedores en los clústeres de Kubernetes. Consulte Supervisar volúmenes contenedores en clústeres de Kubernetes.

Almacenamiento nativo en la nube para administradores de vSphere

Un administrador de vSphere envía recursos de almacenamiento al equipo de Kubernetes y crea directivas de almacenamiento en máquinas virtuales que describen diferentes requisitos de almacenamiento y clases de servicios. Después de aprovisionar cargas de trabajo de Kubernetes con almacenamiento persistente, el administrador de vSphere puede supervisar el ciclo de vida de los recursos de almacenamiento de respaldo y su cumplimiento de los requisitos.

Requisitos de Almacenamiento nativo en la nube

El entorno y las máquinas virtuales de Almacenamiento nativo en la nube que participan en el clúster de Kubernetes deben cumplir con varios requisitos.

Requisitos de Almacenamiento nativo en la nube

- vSphere 6.7 Update 3 o una versión posterior.
- Una versión compatible de Kubernetes.
- Un clúster de Kubernetes implementado en las máquinas virtuales. Para obtener más información sobre cómo implementar el complemento CSI de vSphere y ejecutar el clúster de Kubernetes en vSphere, consulte la documentación sobre la implementación del controlador en GitHub.

Requisitos de máquinas virtuales de clústeres de Kubernetes

- Máquinas virtuales con la versión de hardware 15 o posterior. Instale VMware Tools en cada máquina virtual del nodo.
- Recomendaciones de hardware de máquina virtual:
  - Configure la CPU y la memoria de forma adecuada en función de los requisitos de carga de trabajo.
  - Utilice el controlador SCSI paravirtual de VMware para el disco principal en la máquina virtual del nodo.
- Todas las máquinas virtuales deben poder acceder a un almacén de datos compartido, como vSAN.
- Establezca el parámetro `disk.EnableUUID` en cada máquina virtual del nodo. Consulte Configurar máquinas virtuales de clúster de Kubernetes.
- Para evitar errores y un comportamiento impredecible, no tome instantáneas de las máquinas virtuales de nodo de CNS.

Requisitos del volumen de archivos de CNS

- Utilice vSphere versión 7.0 o posterior con una versión de Kubernetes compatible.
- Use una versión compatible de CSI. Para obtener información, consulte la documentación del controlador de Kubernetes vSphere CSI en GitHub.
- Habilite y configure el servicio de archivos de vSAN. Deberá configurar los dominios, grupos de direcciones IP, red, etc. que sean necesarios del servicio de archivos. Para obtener información, consulte el documento *Administrar VMware vSAN*.
- Siga las directrices específicas para configurar el acceso a la red desde un sistema operativo invitado en el nodo de Kubernetes a un recurso compartido de archivos de vSAN. Consulte Configurar acceso a la red para recurso compartido de archivos de vSAN.

Configurar acceso a la red para recurso compartido de archivos de vSAN

Para poder aprovisionar volúmenes persistentes de ReadWriteMany en el entorno de vSphere Kubernetes genérico, configure las redes, los conmutadores y los enrutadores necesarios de los nodos de Kubernetes en la red del servicio de archivos de vSAN.

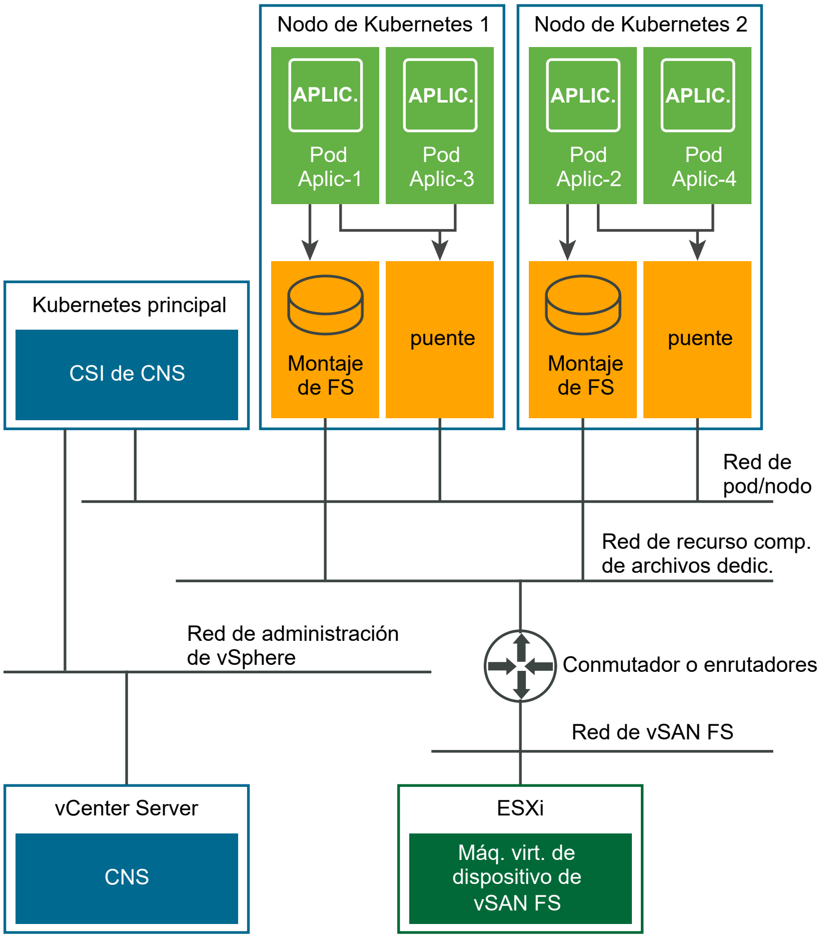
Configurar la red

Siga estos requisitos al configurar las redes:

- En cada nodo de Kubernetes, puede utilizar una vNIC dedicada para el tráfico del recurso compartido de archivos de vSAN. Esta opción solo es necesaria si desea utilizar una ruta de acceso de tráfico de datos segura para los volúmenes de archivos.
- Si utiliza una vNIC dedicada, asegúrese de que el tráfico a través de la vNIC dedicada se pueda enrutar a una o varias redes de servicio de archivos de vSAN.
- Asegúrese de que solo el sistema operativo invitado de cada nodo de Kubernetes pueda acceder directamente al recurso compartido de archivos de vSAN a través de la dirección IP del recurso compartido de archivos. Los pods del nodo no pueden hacer ping ni acceder al recurso compartido de archivos de vSAN a través de su dirección IP.

  El controlador CSI de CNS garantiza que solo los pods que están configurados para usar el volumen de archivos de CNS pueden acceder al recurso compartido de archivos de vSAN mediante la creación de un punto de montaje en el sistema operativo invitado.
- Evite crear un conflicto de direcciones IP entre las máquinas virtuales del nodo y los recursos compartidos de archivos de vSAN.

En la siguiente ilustración se muestra un ejemplo de configuración de red de CNS con el servicio de recurso compartido de archivos de vSAN.



En la ilustración, la configuración de redes de ejemplo sigue estas directrices.

- La configuración utiliza redes independientes para diferentes elementos en el entorno de CNS.

Red	Descripción
Red de administración de vSphere	Por lo general, en un clúster de Kubernetes genérico, cada nodo tiene acceso a esta red.
Red de nodo o pod	Kubernetes utiliza esta red en la comunicación de nodo a nodo y de pod a pod.
Red de recurso compartido de archivos dedicada	El tráfico de datos del volumen de archivos de CNS utiliza esta red.
Red de recurso compartido de archivos de vSAN	Red en la que el recurso compartido de archivos de vSAN está habilitado y donde están disponibles los recursos compartidos de archivos.

- Cada nodo de Kubernetes tienen una vNIC dedicada para el tráfico de archivos. Esta vNIC es independiente de la vNIC que se utiliza para la comunicación de nodo a nodo y de pod a pod. Esta configuración solo se utiliza a modo de ejemplo, pero no es obligatoria.

- Solo las aplicaciones que están configuradas para usar el recurso compartido de archivos de CNS tienen acceso a los recursos compartidos de archivos de vSAN a través del punto de montaje en el sistema operativo invitado del nodo. Por ejemplo, en la ilustración, sucede lo siguiente:
  - Los pods Aplic-1 y Aplic-2 están configurados para usar un volumen de archivos, y tienen acceso al recurso compartido de archivos a través del punto de montaje creado por el controlador CSI.
  - Aplic-3 y Aplic-4 no están configurados con un volumen de archivos, y no pueden acceder a los recursos compartidos de archivos.
- Los recursos compartidos de archivos de vSAN se implementan como contenedores en una máquina virtual de dispositivo de recurso compartido de archivos de vSAN en el host ESXi. Un implementador de Kubernetes, que es un software o un servicio capaz de configurar, implementar y administrar clústeres de Kubernetes, configura los enrutadores y los conmutadores necesarios para que el sistema operativo invitado en el nodo de Kubernetes pueda acceder a los recursos compartidos de archivos de vSAN.

Limitaciones de seguridad

A pesar de que la vNIC dedicada impide que un pod no autorizado acceda directamente a los recursos compartidos de archivos, existen ciertas limitaciones de seguridad:

- La funcionalidad del archivo de CNS da por hecho que cualquiera que tenga el identificador de volumen de archivo de CNS es un usuario autorizado del volumen. Por lo tanto, cualquier usuario que tenga ese identificador de volumen de archivo de CNS podrá acceder a los datos almacenados en el volumen.
- El volumen de archivos de CNS solo admite la autenticación de AUTH_SYS, que es una autenticación basada en identificadores de usuario. Para proteger el acceso a los datos en el volumen de archivos de CNS, se deben utilizar los identificadores de usuario adecuados correspondientes a los contenedores que acceden al volumen de archivos de CNS.
- Un volumen persistente de ReadWriteMany sin enlazar que hace referencia a un volumen de archivos de CNS se puede enlazar mediante una notificación de volumen persistente creada por cualquier usuario de Kubernetes en cualquier espacio de nombres. Asegúrese de que solo los usuarios autorizados tienen acceso a Kubernetes para evitar problemas de seguridad.

Configurar el controlador CSI para acceder a clústeres de servicios de archivos de vSAN

En función de la configuración, el controlador CSI puede aprovisionar volúmenes de archivos en uno o varios clústeres de vSAN donde el servicio de archivos esté habilitado.

Se puede restringir el acceso a únicamente los clústeres de vSAN específicos donde el servicio de archivos esté habilitado. Al implementar el clúster de Kubernetes, configure el controlador CSI con acceso a los clústeres de vSAN específicos del servicio de archivos. Como resultado, el controlador CSI solo puede aprovisionar los volúmenes de archivos en esos clústeres de vSAN.

En la configuración predeterminada, el controlador CSI utiliza cualquier clúster de vSAN del servicio de archivos que haya disponible en vCenter Server para aprovisionar volúmenes de archivos. El controlador CSI no comprueba qué clúster de vSAN del servicio de archivos está accesible mientras se aprovisionan volúmenes de archivos.

Funciones y privilegios de Almacenamiento nativo en la nube

El usuario de vSphere de CNS debe tener privilegios específicos para realizar operaciones relativas al Almacenamiento nativo en la nube.

Puede crear varias funciones para asignar conjuntos de permisos en los objetos que participan en el entorno de Almacenamiento nativo en la nube.

Nota Estas funciones solo se deben crear para clústeres genéricos de Kubernetes. Si trabaja en el entorno de vSphere with Tanzu, utilice la función de administrador de almacenamiento de cargas de trabajo para las operaciones de almacenamiento.

Para obtener más información sobre las funciones y los permisos en vSphere, y acerca de cómo crear una función, consulte la documentación sobre *Seguridad de vSphere*.

Nombre de función.	Nombre del privilegio	Descripción	Necesario para
CNS-Datastore	Almacén de datos > Operaciones de archivos de bajo nivel	Permite realizar tareas de lectura, escritura, eliminación y cambio de nombre en el explorador del almacén de datos.	Almacén de datos compartido en el que residen volúmenes persistentes.
CNS-HOST-CONFIG-STORAGE	Host > Configuración > Configuración de la partición de almacenamiento	Permite la administración de almacenes de datos de vSAN.	Se requiere en un clúster de vSAN con el servicio de archivos de vSAN. Solo se requiere para el volumen de archivos.
CNS-VM	Máquina virtual > Cambiar configuración > Agregar un disco existente	Permite agregar un disco virtual existente a una máquina virtual.	Todas las máquinas virtuales del nodo del clúster.
	Máquina virtual > Cambiar configuración > Agregar o quitar dispositivo	Permite agregar o eliminar cualquier dispositivo que no sea un disco.	
CNS-SEARCH-AND-SPBM	CNS > Permite búsquedas	Permite al administrador de almacenamiento ver la interfaz de usuario de almacenamiento nativo en la nube.	vCenter Server raíz.

Nombre de función.	Nombre del privilegio	Descripción	Necesario para
	Profile-Driven Storage > Vista de Profile-Driven Storage	Permite ver las directivas de almacenamiento definidas.	
Solo lectura	Función predeterminada	Los usuarios con la función Solo lectura para un objeto tienen permiso de ver el estado y los detalles del objeto. Por ejemplo, los usuarios con esta función encontrarán que todas las máquinas virtuales del nodo pueden acceder al almacén de datos compartido. Para los entornos con reconocimiento de zona y topología, todos los antecesores de máquinas virtuales de nodo, como un host, un clúster o un centro de datos, deben tener la función de solo lectura establecida en el usuario de vSphere configurado para usar el controlador CSI y CCM. Esto es necesario para permitir la lectura de etiquetas y categorías a fin de preparar la topología de los nodos.	Todos los hosts en los que residen las máquinas virtuales de los nodos Centro de datos

Crear una directiva de almacenamiento para Kubernetes

El objeto de almacenamiento de vSphere que respaldará a una aplicación en contenedor de Kubernetes debe cumplir unos requisitos de almacenamiento concretos. Como usuario de vSphere, debe crear una directiva de almacenamiento de máquinas virtuales con base en los requisitos que le haya proporcionado el usuario de Kubernetes.

La directiva de almacenamiento se asociará con el disco virtual o el recurso compartido de archivos de vSAN que respalda al contenedor de Kubernetes.

Si cuenta con varias instancias de vCenter Server en el entorno, cree la directiva de almacenamiento de máquinas virtuales en cada instancia. Utilice el mismo nombre de directiva en todas las instancias.

Requisitos previos

- El usuario de Kubernetes identifica el clúster de Kubernetes en el que se implementará la aplicación en contenedor con estado.

- El usuario de Kubernetes recopila los requisitos de almacenamiento relativos a la aplicación en contenedor y los comunica al usuario de vSphere.
- Privilegios necesarios: **Directivas de almacenamiento de máquina virtual. Actualizar** y **Directivas de almacenamiento de máquina virtual. Ver**.

Procedimiento

1 En vSphere Client, abra el asistente **Crear directiva de almacenamiento de máquina virtual**.

   a Haga clic en **Menú > Directivas y perfiles**.

   b En **Directivas y perfiles**, haga clic en **Directivas de almacenamiento de máquina virtual**.

   c Haga clic en **Crear**.

2 Introduzca el nombre y la descripción de la directiva, y haga clic en **Siguiente**.

Opción	Acción
vCenter Server	Seleccione la instancia de vCenter Server.
Nombre	Introduzca el nombre de la directiva de almacenamiento (por ejemplo, `Con uso eficiente del espacio`).
Descripción	Introduzca la descripción de la directiva de almacenamiento.

3 En la sección Reglas específicas del almacén de datos de la página **Estructura de directiva**, seleccione **Habilitar reglas para el almacenamiento de vSAN** y haga clic en **Siguiente**.

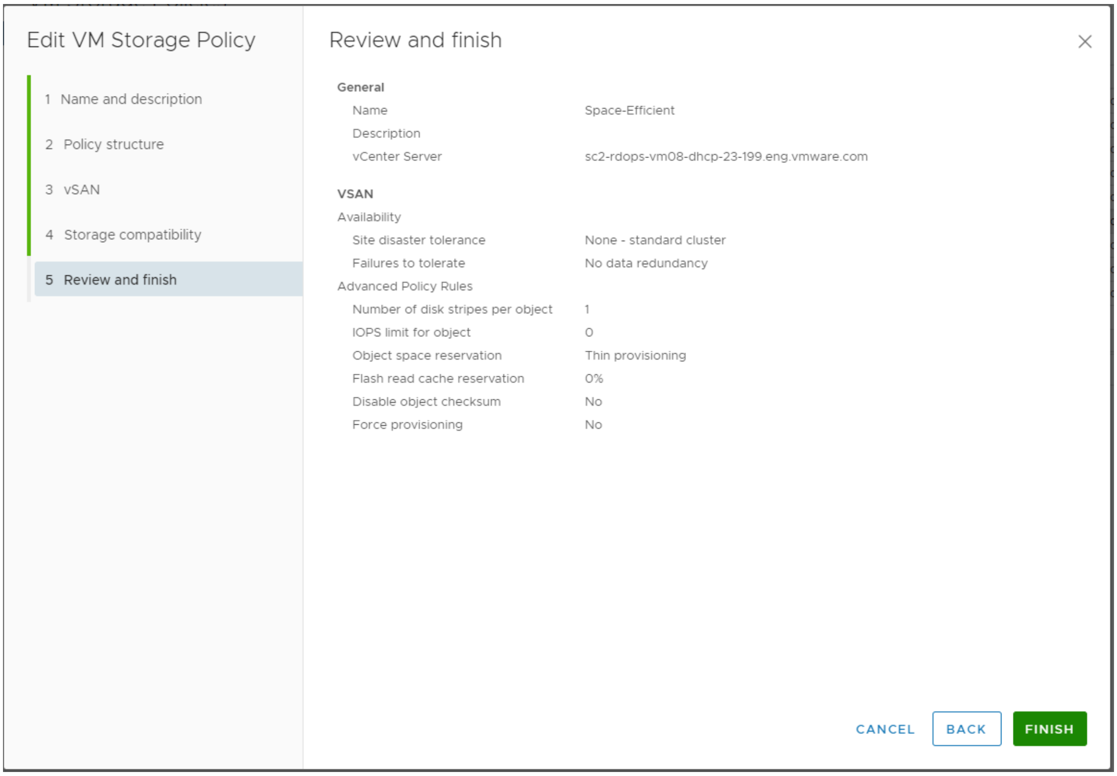
4 En la página **vSAN**, defina el conjunto de reglas de la directiva y haga clic en **Siguiente**.

   a En la pestaña **Disponibilidad**, defina las opciones **Tolerancia ante desastres de sitio** y **Errores que se toleran**.

   b En la pestaña **Reglas de directivas avanzadas**, defina las reglas de directivas avanzadas, como el número de fracciones de disco por objeto y la reserva de Flash Read Cache.

5 En la página **Compatibilidad de almacenamiento**, revise la lista de almacenes de datos de vSAN que coinciden con esta directiva y haga clic en **Siguiente**.

6 En la página **Revisar y finalizar**, revise la configuración de la directiva y haga clic en **Finalizar**.



Pasos siguientes

Ahora puede informar del nombre de la directiva de almacenamiento al usuario de Kubernetes. La directiva de almacenamiento de máquina virtual que creó se utilizará como parte de la definición de clase de almacenamiento del aprovisionamiento dinámico de volúmenes.

Configurar máquinas virtuales de clúster de Kubernetes

En cada máquina virtual del nodo, habilite el parámetro disk.EnableUUID para que las máquinas virtuales se puedan montar correctamente en los discos virtuales.

Siga estos pasos en cada uno de los nodos de máquina virtual que participan en el clúster.

Requisitos previos

- Cree varias máquinas virtuales para el clúster de Kubernetes. Para conocer los requisitos de máquina virtual, consulte Requisitos de Almacenamiento nativo en la nube.
- Privilegio necesario: **Máquina virtual. Configuración. Opciones**.

Nota Para evitar errores y un comportamiento impredecible, no tome instantáneas de las máquinas virtuales de nodo de CNS.

Procedimiento

1 En vSphere Client, haga clic con el botón secundario en la máquina virtual y seleccione **Editar configuración**.

2 Haga clic en la pestaña **Opciones de máquina virtual** y expanda el menú **Opciones avanzadas**.

3 Haga clic en **Editar configuración** junto a Parámetros de configuración.

4 Configure el parámetro **`disk.EnableUUID`**.

Si el parámetro existe, asegúrese de que su valor esté establecido como True. Si no existe, agréguelo y establezca su valor como True.

Nombre	Valor
`disk.EnableUUID`	True

Supervisar volúmenes contenedores en clústeres de Kubernetes

Después de que una aplicación con estado se implemente en Kubernetes, los volúmenes y sus objetos de almacenamiento de vSphere de respaldo se pueden ver en vSphere Client. Puede mostrar y supervisar los volúmenes, así como solucionar los posibles problemas de almacenamiento.

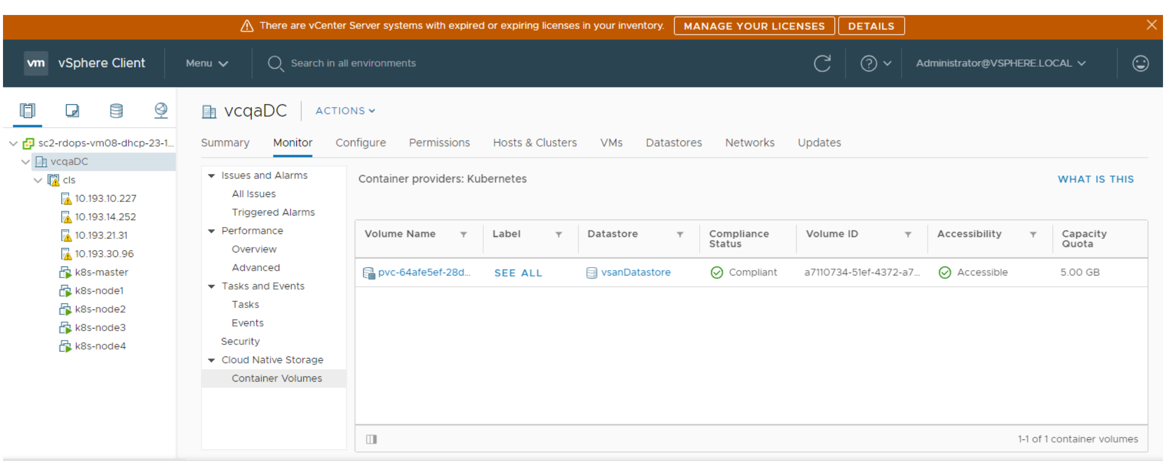
Nota Si se producen errores en el servidor de CNS de Kubernetes, es posible que los objetos de CNS en vSphere Client no se muestren correctamente hasta que se produzca la sincronización completa.

Procedimiento

1 Desplácese hasta la instancia de vCenter Server, un centro de datos o un almacén de datos.

2 Haga clic en la pestaña **Supervisar** y, a continuación, haga clic en **Volúmenes contenedores** en **Almacenamiento nativo en la nube**.

3 Observe los volúmenes contenedores disponibles en su entorno y supervise el estado de cumplimiento de la directiva de almacenamiento de estos.

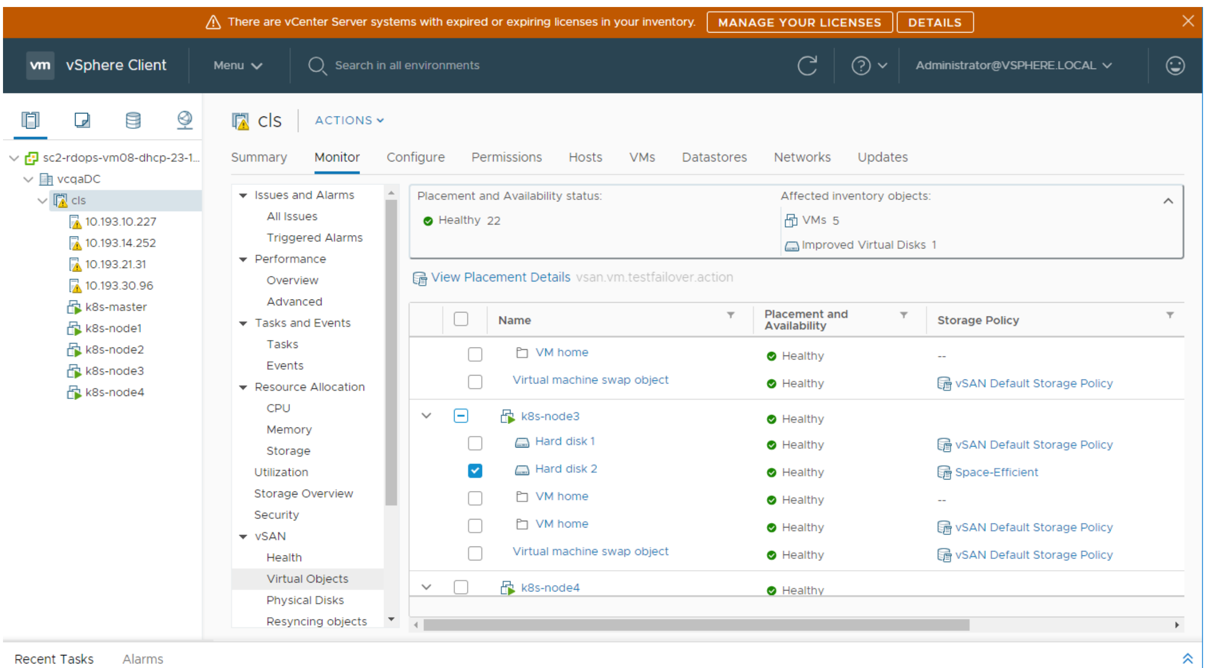


4 Para obtener más detalles, haga clic en el vínculo **VER TODO** de la columna Etiqueta.

Los detalles incluyen el nombre de PersistentVolumeClaim, StorageClass, etc., y ayudan a asignar el volumen a los objetos de Kubernetes asociados a este.

5 Haga clic en el vínculo de la columna **Nombre de volumen** para revisar los distintos componentes que respaldan el volumen, además de detalles como la colocación, el cumplimiento y la directiva de almacenamiento.

Nota La pantalla **Objetos virtuales** está disponible únicamente cuando el almacén de datos subyacente es vSAN.



Usar cifrado con almacenamiento nativo en la nube

A partir de vSphere 7.0, puede utilizar la tecnología de cifrado de vSphere para proteger los discos virtuales de FCD que respaldan los volúmenes persistentes.

El uso del cifrado en el entorno de vSphere requiere preparación e implica configurar una conexión de confianza entre vCenter Server y un proveedor de claves. vCenter Server puede recuperar las claves del proveedor de claves, si fuera necesario. Para obtener información sobre los componentes que participan en el proceso de cifrado de vSphere, consulte Componentes de cifrado de máquinas virtuales de vSphere en la documentación de *Seguridad de vSphere*.

Procedimiento

1 Configure el proveedor de claves en el entorno de vSphere.

Para obtener información, consulte Configurar el clúster del servidor de administración de claves.

2 Cifre todas las máquinas virtuales de nodo del clúster de Kubernetes.

Utilice vSphere Client para realizar este paso.

a Desplácese hasta una máquina virtual de nodo.

b En el menú contextual, seleccione **Directivas de máquina virtual > Editar directivas de almacenamiento de máquina virtual**.

c En el menú desplegable **Directiva de almacenamiento de máquina virtual**, seleccione **Directiva de cifrado de máquina virtual** y haga clic en **Aceptar**.

Para agilizar el proceso de cifrado de las máquinas virtuales de nodo, se puede cifrar únicamente el inicio de la máquina virtual.

3 Cree volúmenes persistentes cifrados en el clúster de Kubernetes con la configuración de CSI de vSphere.

a Cree un objeto StorageClass que haga referencia a la directiva de almacenamiento de cifrado de máquina virtual.

Utilice el siguiente archivo YAML como ejemplo.

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: encryption
provisioner: csi.vsphere.vmware.com
parameters:
  storagePolicyName: "VM Encryption Policy"
  datastore: vsanDatastore
```

b Utilice el objeto PersistentVolumeClaim para aprovisionar el volumen persistente.

PersistentVolumeClaim debe incluir el nombre de la clase de almacenamiento de cifrado en el campo `storageClassName`.

Usar vmkfstools

27

`vmkfstools` es uno de los comandos de ESXi Shell para administrar volúmenes de VMFS, dispositivos de almacenamiento y discos virtuales. Es posible realizar muchas operaciones de almacenamiento con el comando `vmkfstools`. Por ejemplo, puede crear y administrar almacenes de datos de VMFS en una partición física, o manipular archivos de disco virtual, almacenados en almacenes de datos NFS o VMFS.

Nota Después de hacer un cambio con `vmkfstools`, es posible que vSphere Client no se actualice inmediatamente. Utilice una operación de actualización o reexaminación desde el cliente.

Para obtener más información sobre ESXi Shell, consulte *Introducción a ESXCLI*.

Este capítulo incluye los siguientes temas:

Sintaxis del comando vmkfstools

Por lo general, no debe iniciar sesión como usuario raíz para ejecutar los comandos `vmkfstools`. Sin embargo, algunos comandos, como los comandos del sistema de archivos, pueden requerir un inicio de sesión con el usuario raíz.

El comando `vmkfstools` admite la siguiente sintaxis de comandos:

`vmkfstools` *options target*.

El destino especifica una partición, un dispositivo o una ruta de acceso donde aplicar la opción de comando.

Tabla 27-1. Argumentos del comando `vmkfstools`

Argumento	Descripción
opciones	Una o más opciones de líneas de comandos y los argumentos asociados que se utilizan para especificar la actividad que `vmkfstools` realizará. Por ejemplo, se selecciona el formato de disco al crear un nuevo disco virtual. Después de introducir la opción, especifique el destino en el cual se realizará la operación. El destino puede indicar una partición, un dispositivo o una ruta de acceso.
partition	Especifica particiones de discos. Este argumento usa un formato *disk_ID:P*, donde *disk_ID* es el identificador del dispositivo que arroja la matriz de almacenamiento, y *P* es un número entero que representa el número de partición. El dígito de la partición debe ser mayor que cero (0) y debe corresponder a una partición VMFS válida.
device	Especifica dispositivos o volúmenes lógicos. Este argumento utiliza una ruta de acceso en el sistema de archivos del dispositivo ESXi. El nombre de la ruta de acceso comienza con `/vmfs/devices`, que es el punto de montaje del sistema de archivos del dispositivo. Use los siguientes formatos al especificar diferentes tipos de dispositivos: ■ `/vmfs/devices/disks` para discos locales o basados en SAN. ■ `/vmfs/devices/lvm` para volúmenes lógicos de ESXi. ■ `/vmfs/devices/generic` para dispositivos SCSI genéricos.

path	Especifica un sistema de archivos o archivo VMFS. Este argumento es una ruta de acceso absoluta o relativa que nombra a un vínculo simbólico de directorio, una asignación de dispositivo sin formato o un archivo en `/vmfs`.
	■ Para especificar un sistema de archivos VMFS, use este formato:
	`/vmfs/volumes/file_system_UUID`
	o
	`/vmfs/volumes/file_system_label`
	■ Para especificar un archivo en un almacén de datos de VMFS, use este formato:
	`/vmfs/volumes/file_system_label|file_system_UUID/[dir]/myDisk.vmdk`
	Si el directorio de trabajo actual es el directorio principal de `myDisk.vmdk`, no escriba la ruta de acceso completa.

Las opciones del comando vmkfstools

El comando `vmkfstools` tiene varias opciones. Algunas de las opciones se recomiendan solo para usuarios avanzados.

Las formas largas y de letras únicas de las opciones son equivalentes. Por ejemplo, los siguientes comandos son idénticos.

```
vmkfstools --createfs vmfs6 --blocksize 1m disk_ID:P
vmkfstools -C vmfs6 -b 1m disk_ID:P
```

Subopción -v

La subopción `-v` indica el nivel de detalle del resultado del comando.

El formato de esta subopción es el siguiente:

```
-v --verbose number
```

Especifica el valor *number* como un valor entero de 1 a 10.

Puede especificar la subopción `-v` con cualquier opción `vmkfstools`. Si el resultado de la opción no es adecuado para su uso con la subopción `-v`, `vmkfstools` ignora `-v`.

Nota Dado que puede incluir la subopción `-v` en cualquier línea de comando `vmkfstools`, `-v` no se incluye como una subopción en las descripciones de las opciones.

Opciones del sistema de archivos

Las opciones del sistema de archivos permiten crear y administrar almacenes de datos de VMFS. Estas opciones no se aplican a NFS. Puede realizar varias de estas tareas a través de vSphere Client.

Mostrar atributos de un almacén de datos de VMFS

Utilice el comando `vmkfstools` para enumerar los atributos de un almacén de datos de VMFS.

```
-P|--queryfs
      -h|--humanreadable
```

Cuando utiliza esta opción en cualquier archivo o directorio que reside en un almacén de datos de VMFS, la opción enumera los atributos del almacén de datos especificado. Los atributos enumerados generalmente incluyen la etiqueta del sistema de archivos, la cantidad de extensiones del almacén de datos, el UUID y una lista de los dispositivos donde reside cada extensión.

Nota Si cualquier dispositivo que respalda el sistema de archivos VMFS se queda sin conexión, la cantidad de extensiones y de espacio disponible cambiará de manera acorde.

Puede especificar la subopción `-h|--humanreadable` con la opción `-P`. Si lo hace, `vmkfstools` enumerará la capacidad del volumen de manera más legible.

Ejemplo: Ejemplo de la enumeración de atributos de VMFS

```
~ vmkfstools -P -h /vmfs/volumes/my_vmfs
VMFS-5.81 (Raw Major Version: 14) file system spanning 1 partitions.
File system label (if any): my_vmfs
Mode: public
Capacity 99.8 GB, 97.5 GB available, file block size 1 MB, max supported file size 62.9 TB
UUID: 571fe2fb-ec4b8d6c-d375-XXXXXXXXXXXX
Partitions spanned (on "lvm"):
        eui.3863316131XXXXXX:1
Is Native Snapshot Capable: YES
```

Crear un almacén de datos de VMFS o una partición temporal

Use el comando `vmkfstools` para crear un almacén de datos de VMFS o una partición temporal.

```
-C|--createfs [vmfs5|vmfs6|vfat]
```

Esta opción crea un almacén de datos de VMFS en la partición de SCSI especificada, por ejemplo, *disk_ID:P*. La partición se convierte en la partición principal del almacén de datos. Para VMFS5 y VMFS6, el único tamaño de bloque disponible es 1 MB.

Es posible especificar las siguientes subopciones con la opción `-C`.

- `-S|--setfsname`: define la etiqueta de volumen en el almacén de datos de VMFS que se está creando. Utilice esta subopción solo con la opción `-C`. La etiqueta que especifica puede tener un máximo de 128 caracteres y no puede contener ningún espacio en blanco al principio o al final.

  Nota vCenter Server admite un límite de 80 caracteres para todas sus entidades. Si el nombre de un almacén de datos supera ese límite, el nombre se acorta cuando se agrega este almacén de datos a vCenter Server.

  Después de definir una etiqueta de volumen puede utilizarla siempre que especifique el almacén de datos de VMFS para el comando `vmkfstools`. La etiqueta de volumen aparece en listados generados por el comando `ls -l` y como vínculo simbólico al volumen de VMFS en el directorio `/vmfs/volumes`.

  Para cambiar la etiqueta de volumen de VMFS, utilice el comando `ln -sf`. Utilice lo siguiente como ejemplo:

  ```
  ln -sf /vmfs/volumes/UUID /vmfs/volumes/datastore
  ```

  datastore es la nueva etiqueta de volumen que se utilizará para el VMFS del *UUID*.

  Nota Si el host está registrado en vCenter Server, vCenter Server sobrescribirá todos los cambios que realice a la etiqueta de volumen de VMFS. Esta operación garantiza que la etiqueta de VMFS sea coherente en todos los hosts de vCenter Server.

- `-Y|--unmapGranularity #[bBsSkKmMgGtT]`: esta subopción se aplica a VMFS6 solamente. Define la granularidad para la operación de anulación de asignación. La granularidad predeterminada es de 1 MB. Como con el tamaño de bloque, introduzca el tipo de unidad.
- `-O|--unmapPriority <none|low|medium|high>`: esta subopción se aplica a VMFS6 solamente. Define la prioridad para la operación de anulación de asignación.

Ejemplo: Ejemplo de creación de un sistema de archivos VMFS

Este ejemplo ilustra la creación de un almacén de datos de VMFS6 con el nombre my_vmfs en la partición `naa.`*`Identificador`*`:1`.

```
~ vmkfstools -C vmfs6 -S my_vmfs /vmfs/devices/disks/naa.ID:1
```

Agregar una extensión a un almacén de datos de VMFS

Use el comando `vmkfstools` para agregar una extensión a un almacén de datos de VMFS.

Cuando se agrega una extensión, se abarca el almacén de datos de VMFS desde la partición principal por toda la partición que especifica *span_partition*.

```
-Z|--spanfs span_partitionhead_partition
```

Debe especificar el nombre de la ruta de acceso completo para las particiones principales y de expansión, por ejemplo `/vmfs/devices/disks/`*`disk_ID:1`*. Cada vez que se usa esta opción, se agrega una extensión al almacén de datos de VMFS, por lo cual el almacén de datos se expande a varias particiones.

Precaución Cuando se ejecuta esta opción, se pierden todos los datos que existían previamente en el dispositivo SCSI que se especificó en *span_partition*.

Ejemplo: Ejemplo para extender un almacén de datos de VMFS

En este ejemplo, se extiende la partición principal existente del almacén de datos de VMFS con una nueva partición.

```
~ vmkfstools -Z /vmfs/devices/disks/naa.disk_ID_2:1 /vmfs/devices/disks/naa.disk_ID_1:1
```

El almacén de datos extendido tiene dos particiones: `naa.`*`disk_ID_1`*`:1` y `naa.`*`disk_ID_2`*`:1`. En este ejemplo, `naa.`*`disk_ID_1`*`:1` es el nombre de la partición principal.

Expansión de un almacén de datos de VMFS

En lugar de agregar una extensión a un almacén de datos de VMFS, puede aumentar el tamaño de un almacén de datos existente. Use el comando `vmkfstools -G`.

Podría aumentar el tamaño del almacén de datos una vez que el almacenamiento subyacente haya aumentado su capacidad.

El comando utiliza la siguiente opción:

```
-G|--growfs devicedevice
```

Esta opción amplía el almacén de datos de VMFS o su extensión específica. Por ejemplo,

```
vmkfstools --growfs /vmfs/devices/disks/disk_ID:1 /vmfs/devices/disks/disk_ID:1
```

Opciones de discos virtuales

Las opciones de disco virtual permiten configurar, migrar y administrar discos virtuales almacenados en los almacenes de datos. También se pueden realizar la mayoría de estas tareas mediante vSphere Client.

Formatos de disco compatibles

Cuando se crea o clona un disco virtual, se puede utilizar la subopción `-d|--diskformat` para especificar el formato del disco.

Elija entre los formatos siguientes:

- `zeroedthick` (predeterminado): el espacio necesario para el disco virtual se asigna durante la creación. Los datos que quedan en el dispositivo físico no se borran durante la creación, sino que se ponen a cero bajo demanda en la primera escritura de la máquina virtual. La máquina virtual no lee los datos obsoletos del disco.
- `eagerzeroedthick`: el espacio necesario para el disco virtual se asigna en el momento de la creación. En contraposición con el formato `zeroedthick`, los datos que quedan en el dispositivo físico se ponen a cero durante la creación. Es posible que la creación de discos en este formato demore mucho más que la creación de otros tipos de discos.
- `thin`: disco virtual de aprovisionamiento fino. A diferencia del formato `thick`, el espacio requerido para el disco virtual no se asigna durante la creación, sino que se proporciona, puesto a cero, bajo demanda.
- `rdm:`*device*: asignación de disco sin formato en modo de compatibilidad virtual.
- `rdmp:`*device*: asignación de disco sin formato (de acceso directo) en modo de compatibilidad física.
- `2gbsparse`: disco disperso con el tamaño máximo de extensión de 2 GB. Se pueden utilizar discos en este formato con productos VMware alojados, como VMware Fusion. Sin embargo, no se puede encender un disco disperso en un host ESXi a menos que primero se vuelva a importar el disco con `vmkfstools` en un formato compatible, como `thick` o `thin`.

Formatos de disco en almacenes de datos NFS

Los únicos formatos de disco que se pueden utilizar para NFS son `thin`, `thick`, `zeroedthick` y `2gbsparse`.

Los formatos `Thick`, `zeroedthick` y `thin`, por lo general, se comportan igual dado que el servidor NFS, y no el host ESXi, determina la directiva de asignación. La directiva de asignación predeterminada en la mayoría de los servidores NFS es `thin`. Sin embargo, en los servidores NFS que admiten Storage APIs - Array Integration, se pueden crear discos virtuales en formato `zeroedthick`. La operación de reserva de espacio habilita los servidores NFS para asignar y garantizar espacio.

Para obtener más información sobre las API de integración de matrices, consulte Capítulo 24 Aceleración de hardware de almacenamiento.

Crear un disco virtual

Utilice el comando `vmkfstools` para crear un disco virtual.

```
-c|--createvirtualdisk size[bB|sS|kK|mM|gG]
          -d|--diskformat [thin|zeroedthick|eagerzeroedthick]
          -W|--objecttype [file|vsan|vvol]
          --policyFile fileName
```

Esta opción crea un disco virtual en la ruta de acceso especificada en un almacén de datos. Especifique el tamaño del disco virtual. Al introducir el valor de *size*, puede indicar el tipo de unidad agregando el sufijo `k` (kilobytes), `m` (megabytes) o `g` (gigabytes). El tipo de unidad no distingue entre mayúsculas y minúsculas. `vmkfstools` interpreta que `k` o `K` significa kilobytes. Si no se especifica un tipo de unidad, `vmkfstools` toma los bytes como valor predeterminado.

Es posible especificar las siguientes subopciones con la opción `-c`.

- `-d|--diskformat` especifica los formatos de disco.
- `-W|--objecttype` especifica si el disco virtual es un archivo de un almacén de datos de VMFS o NFS, o bien un objeto de un almacén de datos vSAN o Virtual Volumes.
- `--policyFile` *`fileName`* especifica la directiva de almacenamiento de máquina virtual para el disco.

Ejemplo: Ejemplo para crear un disco virtual

Este ejemplo muestra cómo crear un disco virtual de dos gigabytes llamado `disk.vmdk`. Cree el disco en el almacén de datos de VMFS llamado `myVMFS`. El archivo de disco representa un disco virtual vacío al que pueden acceder las máquinas virtuales.

```
vmkfstools -c 2048m /vmfs/volumes/myVMFS/disk.vmdk
```

Inicializar un disco virtual

Use el comando `vmkfstools` para inicializar un disco virtual.

```
-w|--writezeros
```

Esta opción limpia el disco virtual sobrescribiendo con ceros todos sus datos. Según el tamaño del disco virtual y el ancho de banda de E/S del dispositivo que aloja el disco virtual, es posible que la ejecución de este comando tarde mucho tiempo.

Precaución Si usa este comando, perderá todos los datos que tenga el disco virtual.

Expandir un disco virtual fino

Utilice el comando `vmkfstools` para expandir un disco virtual fino.

```
-j|--inflatedisk
```

Esta opción convierte un disco virtual `thin` en un disco `eagerzeroedthick`, y conserva todos los datos existentes. Esta opción asigna y llena con ceros todos los bloques que aún no están asignados.

Convertir un disco virtual grueso con algunos bloques puestos a cero a un disco virtual grueso con todos los bloques puestos a cero

Use el comando `vmkfstools` para convertir todos los discos virtuales gruesos con algunos bloques puestos a cero a discos gruesos con todos los bloques puestos a cero.

```
-k|--eagerzero
```

Al realizar esta conversión, esta opción preserva todos los datos presentes en el disco virtual.

Siga este ejemplo:

```
vmkfstools --eagerzero /vmfs/volumes/myVMFS/VMName/disk.vmdk
```

Quitar bloques puestos a cero

Utilice el comando `vmkfstools` para quitar los bloques puestos a cero.

```
-K|--punchzero
```

Esta opción desasigna todos los bloques puestos a cero y deja solo aquellos asignados previamente y con datos válidos. El disco virtual resultante tiene formato fino.

Eliminar un disco virtual

Use el comando vmkfstools para eliminar un archivo de disco virtual en la ruta de acceso especificada del volumen VMFS.

Utilice la siguiente opción:

```
-U|--deletevirtualdisk
```

Cambiar nombre de un disco virtual

Use el comando vmkfstools para cambiar el nombre de un archivo de disco virtual en la ruta de acceso especificada en el volumen VMFS.

Debe especificar el nombre del archivo o la ruta de acceso del archivo original *oldName* y el nombre del archivo o la ruta de acceso del archivo nuevo *newName*.

```
-E|--renamevirtualdisk oldNamenewName
```

Clonar convertir un disco virtual o un RDM

Use el comando vmkfstools para crear una copia de un disco virtual o un disco sin formato que especifique.

Un usuario no raíz no puede clonar un disco virtual o un RDM. Debe especificar el nombre del archivo o la ruta de acceso del archivo original *oldName* y el nombre del archivo o la ruta de acceso del archivo nuevo *newName*.

```
 -i|--clonevirtualdisk oldName newName
      -d|--diskformat [thin|zeroedthick|eagerzeroedthick|rdm:device|rdmp:device|2gbsparse]
      -W|--objecttype [file|vsan|vvol]
      --policyFile fileName
      -N|--avoidnativeclone
```

Use las siguientes subopciones si desea cambiar los parámetros correspondientes para la copia que va a crear.

- `-d|--diskformat` especifica los formatos de disco.
- `-W|--objecttype` especifica si el disco virtual es un archivo de un almacén de datos de VMFS o NFS, o bien un objeto de un almacén de datos vSAN o Virtual Volumes.
- `--policyFile` *`fileName`* especifica la directiva de almacenamiento de máquina virtual para el disco.

De manera predeterminada, ESXi usa sus métodos nativos para realizar las operaciones de clonación. Si la matriz admite las tecnologías de clonación, puede descargar las operaciones para la matriz. Para evitar la clonación nativa de ESXi, especifique la opción `-N|--avoidnativeclone`.

Ejemplo: Ejemplo de clonación o conversión de un disco virtual

En este ejemplo, se ilustra la clonación de contenido de un disco virtual principal del repositorio `templates` a un archivo de disco virtual llamado `myOS.vmdk` en el sistema de archivos `myVMFS`.

```
vmkfstools -i /vmfs/volumes/myVMFS/templates/gold-primary.vmdk /vmfs/volumes/myVMFS/myOS.vmdk
```

Es posible configurar una máquina virtual para que utilice este disco virtual agregando líneas al archivo de configuración de la máquina virtual, como se muestra en el siguiente ejemplo:

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/myOS.vmdk
```

Si quiere convertir el formato del disco, use la subopción `-d|--diskformat`.

Esta subopción resulta útil cuando importa discos virtuales en un formato que no es compatible con ESXi, por ejemplo, el formato 2gbsparse. Después de convertir el disco, puede asociarlo a una nueva máquina virtual que cree en ESXi.

Por ejemplo:

```
vmkfstools -i /vmfs/volumes/myVMFS/templates/gold-primary.vmdk /vmfs/volumes/myVMFS/
myOS.vmdk  -d thin
```

Extender un disco virtual

Después de crear una máquina virtual, puede usar el comando vmkfstools para extender el tamaño de un disco asignado a la máquina virtual.

```
-X|--extendvirtualdisk newSize[bBsSkKmMgGtT]
```

Agregue un sufijo de unidad adecuado para especificar el parámetro `newSize`. El tipo de unidad no distingue entre mayúsculas y minúsculas. `vmkfstools` interpreta que `k` o `K` significa kilobytes. Si no especifica el tipo de unidad, `vmkfstools` toma los kilobytes como valor predeterminado.

El parámetro `newSize` define el tamaño nuevo completo, no solo el incremento que se agrega al disco.

Por ejemplo, para extender un disco virtual de 4 G con 1 G más, escriba: `vmkfstools -X 5g`*disk name*.

Puede ampliar el disco virtual al formato grueso con todos los bloques puestos a cero con la opción `-d eagerzeroedthick`.

Al utilizar la opción `-X`, se deben tener en cuenta las siguientes consideraciones:

- No amplíe el disco base de una máquina virtual con instantáneas asociadas. Si lo hace, ya no podrá confirmar la instantánea ni revertir el disco base al tamaño original.
- Después de extender el disco, es posible que necesite actualizar el sistema de archivos en el disco. Como resultado, el sistema operativo invitado reconoce el nuevo tamaño del disco y puede usarlo.

Actualizar discos virtuales

Esta opción convierte el archivo de disco virtual especificado del formato de ESX Server 2 al formato de ESXi.

Use esta opción para convertir discos virtuales del tipo LEGACYSPARSE, LEGACYPLAIN, LEGACYVMFS, LEGACYVMFS_SPARSE y LEGACYVMFS_RDM.

```
-M|--migratevirtualdisk
```

Crear un modo de compatibilidad virtual con asignación de dispositivos sin formato

Use el comando vmkfstools para crear un archivo de asignación de dispositivos sin formato (Raw Device Mapping, RDM) en un volumen VMFS y asignar un LUN sin formato a este archivo. Una vez establecida esta asignación, se puede acceder al LUN del mismo modo que se accede a un disco virtual VMFS normal. La longitud de archivo de la asignación es igual al tamaño del LUN sin formato al que se apunta.

```
-r|--createrdm device
```

Cuando especifique el parámetro *device*, utilice el siguiente formato:

```
/vmfs/devices/disks/disk_ID:P
```

Ejemplo: Ejemplo para crear un RDM de modo de compatibilidad virtual

En este ejemplo, se crea un archivo RDM denominado *my_ rdm.vmdk* y se asigna el disco sin formato *disk_ ID* a ese archivo.

```
vmkfstools -r /vmfs/devices/disks/disk_ID my_rdm.vmdk
```

Para configurar la máquina virtual para que utilice el archivo de asignación `my_rdm.vmdk`, agregue las líneas siguientes al archivo de configuración de la máquina virtual:

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/my_rdm.vmdk
```

Crear una asignación de dispositivo sin formato de modo de compatibilidad física

Use el comando vmkfstools para asignar un dispositivo sin formato de acceso directo a un archivo en un volumen VMFS. Con la asignación, una máquina virtual puede omitir el filtrado del comando SCSI ESXi al acceder a su disco virtual. Este tipo de asignación es útil cuando la máquina virtual debe enviar comandos SCSI propios, por ejemplo cuando el software basado en SAN se ejecuta en la máquina virtual.

```
-z|--createrdmpassthru deviceejemplo.vmdk
```

Una vez que se establece este tipo de asignación, se puede utilizar para acceder al disco sin formato del mismo modo que se accede a cualquier otro disco virtual VMFS.

Cuando especifique la ruta *device*, utilice el siguiente formato:

```
/vmfs/devices/disks/ID_de_dispositivo
```

Utilice este formato para el nombre del archivo .vmdk. Asegúrese de crear el almacén de datos antes de utilizar el comando.

```
/vmfs/volumes/datastore_name/ejemplo.vmdk
```

Por ejemplo,

```
vmkfstools -z /vmfs/devices/disks/naa.600a0000000000000... /vmfs/volumes/datastore1/
mydisk.vmdk
```

Mostrar atributos de un RDM

Use el comando vmkfstools para enumerar los atributos de una asignación de disco sin formato. Los atributos permiten identificar el dispositivo de almacenamiento al cual se asignan los archivos RDM.

```
-q|--queryrdm my_rdm.vmdk
```

Esta opción imprime el nombre del RDM del disco sin formato. La opción también imprime otra información de identificación, como el identificador de disco, del disco sin formato.

Ejemplo: Ejemplo de la enumeración de atributos de RDM

```
# vmkfstools -q /vmfs/volumes/VMFS/my_vm/my_rdm.vmdk

Disk /vmfs/volumes/VMFS/my_vm/my_rdm.vmdk is a Passthrough Raw Device Mapping

Maps to: vml.020000000060050768019002077000000000000005323134352020
```

Mostrar la geometría del disco virtual

Use el comando vmkfstools para obtener información acerca de la geometría de un disco virtual.

```
-g|--geometry
```

El resultado tiene la siguiente forma: `Geometry information C/H/S`, donde `C` representa la cantidad de cilindros, `H` representa la cantidad de encabezados y `S` representa la cantidad de sectores.

Nota Cuando se importan discos virtuales de los productos VMware alojados en el host ESXi, es posible que aparezca un mensaje de error de falta de coincidencia con la geometría del disco. Una falta de coincidencia con la geometría también puede desencadenar problemas al cargar un sistema operativo invitado o al ejecutar una máquina virtual creada recientemente.

Comprobar y reparar discos virtuales

Use el comando vmkfstools para revisar o reparar un disco virtual si se daña.

```
-x|--fix [check|repair]
```

Por ejemplo,

```
vmkfstools -x check /vmfs/volumes/my_datastore/my_disk.vmdk
```

Comprobar la consistencia de la cadena de discos

Use el comando vmkfstools para revisar toda la cadena de instantáneas. Puede determinar si alguno de los eslabones de la cadena está corrupto o si existe alguna relación de elementos primarios y secundarios no válida.

```
-e|--chainConsistent
```

Opciones de dispositivos de almacenamiento

Puede utilizar las opciones de dispositivos del comando vmkfstools a fin de realizar una tarea administrativa para dispositivos de almacenamiento físico.

Administrar reservas de SCSI de LUN

Utilice el comando vmkfstools para reservar un LUN de SCSI para uso exclusivo del host ESXi. También puede liberar una reserva para que otros hosts tengan acceso al LUN y restablecer una reserva para forzar la liberación de todas las reservas del destino.

```
-L|--lock [reserve|release|lunreset|targetreset|busreset|readkeys|readresv] device
```

Precaución Utilizar la opción `-L` puede interrumpir las operaciones de otros servidores en una SAN. Utilice esta opción `-L` solo durante la solución de problemas de configuración de agrupación en clústeres.

A menos que VMware lo recomiende, jamás utilice esta opción en un LUN que aloje un volumen de VMFS.

Puede especificar la opción `-L` de varias maneras:

- `-L reserve`: reserva el LUN especificado. Después de la reserva, solo el servidor que reservó ese LUN puede acceder a él. Si otros servidores intentan acceder a ese LUN, se muestra un error de reserva.
- `-L release`: libera la reserva en el LUN especificado. Otros servidores pueden volver a acceder al LUN.
- `-L lunreset`: restablece el LUN especificado borrando todas las reservas en el LUN y permitiendo que vuelva a estar disponible para todos los servidores. Esto no afecta a ningún otro LUN del dispositivo. Si otro LUN del dispositivo está reservado, lo seguirá estando.
- `-L targetreset`: restablece todo el destino. Esta acción borra todas las reservas en todos los LUN asociados con ese destino y hace que los LUN vuelvan a estar disponibles para todos los servidores.
- `-L busreset`: restablece todos los destinos accesibles en el bus. Esta acción borra todas las reservas en los LUN accesibles a través del bus y hace que vuelvan a estar disponibles para todos los servidores.

- `-L readkeys`. lee las claves de reserva registradas en un LUN. Se aplica a la funcionalidad de reserva de grupos persistentes de SCSI-III.
- `-L readresv`: lee el estado de reserva de un LUN. Se aplica a la funcionalidad de reserva de grupos persistentes de SCSI-III.

Al introducir el parámetro *device*, utilice el siguiente formato:

```
/vmfs/devices/disks/disk_ID:P
```

Romper el bloqueo de dispositivos

Use el comando vmkfstools para romper el bloqueo del dispositivo en una partición específica.

```
-B|--breaklock device
```

Al introducir el parámetro *device*, utilice el siguiente formato:

```
/vmfs/devices/disks/disk_ID:P
```

Puede utilizar este comando cuando un host genera errores en mitad de una operación del almacén de datos; por ejemplo, expandir el almacén de datos, agregar una extensión o volver a firmar. Al ejecutar este comando, asegúrese de que ningún otro host mantenga el bloqueo.